entropy

MDPI

Article

Sending-or-Not-Sending Twin-Field Quantum Key Distribution with a Passive Decoy-State Method

Ke Xue [1], Zhigang Shen [1], Shengmei Zhao [1,2,*] and Qianping Mao [2,3,*]

[1] Institute of Signal Processing Transmission, Nanjing University of Posts and Telecommunications (NUPT), Nanjing 210003, China; 1019010506@njupt.edu.cn (K.X.); shenzg@126.com (Z.S.)
[2] Key Lab of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing 210003, China
[3] College of Computer Science and Technology, Nanjing Tech University, Nanjing 211816, China
* Correspondence: zhaosm@njupt.edu.cn (S.Z.); maoqp1@njtech.edu.cn (Q.M.)

Abstract: Twin-field quantum key distribution (TF-QKD) has attracted considerable attention because it can exceed the basic rate-distance limit without quantum repeaters. Its variant protocol, sending or not-sending quantum key distribution (SNS-QKD), not only fixes the security vulnerability of TF-QKD, but also can tolerate large misalignment errors. However, the current SNS-QKD protocol is based on the active decoy-state method, which may lead to side channel information leakage when multiple light intensities are modulated in practice. In this work, we propose a passive decoy-state SNS-QKD protocol to further enhance the security of SNS-QKD. Numerical simulation results show that the protocol not only improves the security in source, but also retains the advantages of tolerating large misalignment errors. Therefore, it may provide further guidance for the practical application of SNS-QKD.

Keywords: sending-or-not-sending; passive decoy-state; quantum key distribution

Citation: Xue, K.; Shen, Z.; Zhao, S.; Mao, Q. Sending-or-Not-Sending Twin-Field Quantum Key Distribution with a Passive Decoy-State Method. *Entropy* **2022**, *24*, 662. https://doi.org/10.3390/e24050662

Academic Editors: Xiang-Bin Wang, Cong Jiang and Leong Chuan Kwek

Received: 18 April 2022
Accepted: 6 May 2022
Published: 8 May 2022

1. Introduction

Quantum key distribution (QKD) allows legitimate communicators to share a common key based on the laws of quantum physics [1–3]. Thus far, QKD has been developed for nearly 40 years, and great progress has been made both theoretically and experimentally. The emergence of excellent protocols, such as the BB84 protocol [4], Measurement-Device-Independent QKD (MDI-QKD) protocol [5–9] and Round-Robin Differential-Phase-Shift QKD (RRDPS-QKD) protocol [10–12], has promoted the progress of QKD. Unfortunately, the above protocols have not broken through the basic rate-distance limit of repeaterless QKD, which is called the PLOB bound [13].

In 2018, the revolutionary twin-field quantum key distribution (TF-QKD) protocol proposed by Lucanarini et al. [14] was able to effectively overcome the PLOB bound, and its experimental secure transmission distance even exceeded 500km. Then, many variant QKD protocols and further studies [15–22] followed to develop the performance of TF-QKD. As the protocol with the longest transmission distance in current QKD experiments, sending-or-not-sending TF-QKD (SNS-QKD) [15,23–30] not only fixes the security vulnerability of TF-QKD, but also tolerates large misalignment errors. Since the single-photon interference is not needed in the signal window [15], SNS-QKD is more practical than other TF-QKD variant protocols.

The QKD systems always adopt the decoy-state method [31–35] to tackle photon-number-splitting (PNS) attacks [36,37], so as to guarantee the security of the light source. Usually, different intensities are actively modulated by the acousto- or electro-optic modulators on the light sources in experiments. Although active modulation is sufficient to achieve decoy-state SNS-QKD, passive modulation of the pulse is still necessary in some cases—for instance, when the intensity modulator is not properly designed so that some

physical parameters of the emitted pulses depend on the particular setting [38]. Thus, the active modulation of the pulse intensity at this time will cause severe security problems [38]. Thus far, passive decoy-state methods have been proposed [39–43] and verified [7,44] to be able to reduce the information leakage. However, SNS-QKD using the passive decoy-state method has not been proposed.

Here, in this work, we propose a passive decoy-state SNS-QKD scheme to further improve the security of SNS-QKD in a light source. The scheme uses the heralded single-photon source (HSPS) [45] as a signal source, while the weak coherent state source (WCSs) is still used as a decoy source. The authorized user Alice (or Bob) passively selects whether it is a signal window or a decoy window according to the local detection events occurring at her (his) side. In addition, we compare the performance of the passive scheme with the original SNS-QKD under different conditions, and it is indicated that the proposed protocol retains all the advantages of the original SNS-QKD.

The paper is arranged as follows. In Section 2, we describe the content of our protocol and its settings. We analyze the security of the passive decoy-state method SNS protocol in Section 3 and give the method of calculating the key rate in Section 4. In Section 5, we present the numerical simulation and give an analysis of the these results. Finally, the conclusion is given in Section 6.

2. Passive Decoy-State SNS-QKD Protocol

Before introducing our protocol, some assumptions are clarified. First of all, Alice, Bob and Charlie are completely isolated. Secondly, the path of local detection is much shorter than mode S and mode D.

The schematic diagram of passive decoy-state SNS-QKD is shown in Figure 1. Firstly, the pulses are split into two modes (mode D and mode S) by BS1. The mode D is used to send decoy-state pulses, and mode S is used to send signal-state pulses. Next, Alice and Bob passively select one of the modes according to local detection. If Alice (Bob) selects mode D (mode S), she (he) will use the VOA to attenuate the mode S (mode D) pulses. After the pulses are interfered by BS, Charlie announces the results of the successful events. Then, Alice and Bob extract the sifted keys according to the published measurement results. Finally, Alice and Bob can share a secure key after performing error correction and private amplification. The detailed steps of our passive decoy-state SNS-QKD scheme can be described as follows.

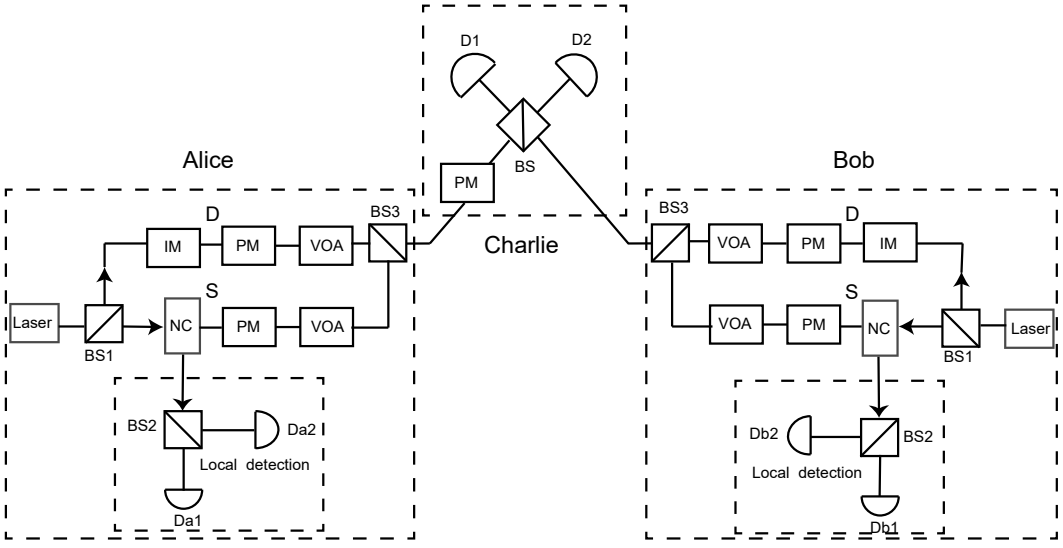

Figure 1. The settings of the passive decoy-state SNS-QKD protcol. BS, beam splitter; IM, intensity modulator; PM, phase modulator; VOA, variable optical attenuator; NC, nonlinear crystal; Local detection, a beam splitter and two local single-photon detectors (Da1 and Da2, Db1 and Db2); D1 and D2, single-photon detectors at Charlie side.

Step 1: First of all, the pulses are split into two modes (mode D and mode S) by BS1. The mode D adopts the weak coherent state sources (WCSs) while the mode S adopts the heralded single-photon source (HSPS). The pulses of mode D are modulated by an intensity modulator (IM) and encoded by a phase modulator (PM). The pulses of mode S are further separated into two parts through the parametric down-conversion (PDC) process of the NC. One part (local detection) consists of a beam splitter and two local detectors, and the pulses of another part are then encoded by a phase modulator (PM).

Step 2: Alice (Bob) passively selects whether it is a signal window or a decoy window based on the local detector events. When it is a decoy window, Alice (Bob) randomly chooses one from a few decoy states $\left|\mu_m e^{i\theta_a}\right\rangle$ ($\left|\mu_m e^{i\theta_b}\right\rangle$) ($\mu_m \in \mu, v, 0$), which are WCSs. When it is a signal window, Alice (Bob) normally decides to send a signal pulse (HSPS) with a random phase shift θ_a (θ_b) by probability ϵ, and she (he) decides to attenuate the pulse by probability $1-\epsilon$ after the detector click.

Note that, as shown in Table 1, the local detection events can be divided into four types, denoted as E_i (i = 1, 2, 3, 4), corresponding to (1) no response, (2) only Da1 (Db1) response, (3) only Da2 (Db2) response, (4) both responses. Apparently, Alice (Bob) can use these four detection events to passively select whether it is a decoy window or a signal window. After Alice and Bob select the corresponding window, they will use the VOA to attenuate the pulses of the other window. For example, if Alice (Bob) chooses the signal window, she (he) can attenuate the decoy window pulses with a VOA. Moreover, the operation of 'not sending' a pulse in the original SNS-QKD [15] is no longer applicable in our protocol because, if no pulse is sent, there will be no local detection event response. Hence, in order to maintain the security equivalence with the original SNS-QKD, we use VOA to attenuate the pulse to zero output to represent the 'not sending' operation so as to maintain the completeness of the protocol.

Table 1. Definition of various detection events. Taking Alice side as an example, 0 indicates that the detector has not clicked, and 1 indicates that the detector has clicked.

Events	Da1	Da2
E_1	0	0
E_2	1	0
E_3	0	1
E_4	1	1

Step 3: Charlie measures the incoming pulses with a BS and announces the measurement results.

Step 4: After the interference by BS, Alice and Bob announce the local detection events and the extra phase of the decoy window.

Note that successful events are defined as the following two situations: (a) both Alice and Bob select the corresponding signal window, and only one detector clicks on Charlie's side; (b) when Charlie announces that only one detector clicks, Alice and Bob both select the corresponding decoy window, and phases θ_a, θ_b satisfy one of the following two equations:

$$|\theta_a - \theta_b| \leq \frac{2\pi}{M}, |\theta_a - \theta_b - \pi| \leq \frac{2\pi}{M}, \tag{1}$$

where M refers to the total number of phase slices pre-chosen by Alice and Bob.

Step 5: Alice and Bob take some post-processing measures such as error correction and privacy amplification to extract the secure key.

3. The Security Analysis

It is known that our protocol maintains most parts of the original SNS protocol except that the active decoy-state method is replaced by the passive-decoy state method. Therefore,

we only need to analyze the security problems that are caused by this difference from the original SNS-QKD. Here, we discuss them individually as follows.

(i) The HSPS. In order to implement the passive decoy-state method, we use the HSPS to replace the WCSs of the original SNS in the signal window. Compared with WCPs, the HSPS has a larger single-photon component and smaller vacuum component, which has better performance in the QKD protocol. Many experiments have developed their applications [46,47] with HSPS. The SNS-QKD protocol with the HSPS was further discussed in Ref. [30]. Therefore, the replacement of HSPS will not cause security vulnerabilities of our protocol.

(ii) The passive decoy-state method. Many successful implementations of the passive decoy-state technique in QKD experiments show that it is practical and feasible for the passive decoy-state method [7,44]. Compared with the active decoy-state method, the passive decoy-state method selects the signal state and the decoy state according to the local detection events. This approach not only does not have security vulnerabilities but also improves the security of the protocol. Firstly, the passive decoy-state method can also resist PNS attacks as the eavesdropper cannot distinguish whether the pulse is in the decoy state or signal state. Secondly, it can avoid the security vulnerabilities caused by actively modulating the intensity of the source. For example, Jiang et al. proposed an attack called wavelength-selected photon-number-splitting (WSPNS) in 2012. This attack uses the frequency factor introduced by intensity modulation to distinguish the signal state and decoy state. However, the proposed scheme uses local detection events to distinguish the signal states and decoy states. Therefore, we can make the signal state intensity (laser intensity) the same as one of the decoy state. When both the signal-state intensity and the decoy-state intensity are same (for instance, both intensities are μ), intensity modulation is no longer required. For the vacuum decoy state, the frequency cannot be introduced because there is no pulse. Since there are two decoy states that cannot be distinguished, the WSPNS attack will become ineffective.

(iii) Attenuation of the pulses. In our protocol, the choice of signal state and decoy state needs to be determined according to the response of the local detector. Therefore, we use the VOA to attenuate the pulses instead of not sending pulses. Although the imperfections of the VOA device will decrease the key generation rate of our protocol, it does not leak any information. Thus, attenuation of the pulses has no impact on the security. Additionally, one can reduce the key rate decrease in the post-processing stage.

4. The Key Rate

In this part, we will discuss the key rate of the passive decoy-state method SNS-QKD.

4.1. The Probability Distribution

In this protocol, we need to deduce the corresponding probability distribution of E_1 event to analyze the key rate. Following the previous works on QKD with the passive decoy-state method [41,42], we give a brief overview of the derivation process as follows.

Taking the Alice side as an example, suppose that d_1 and d_2 are the dark counts of the two local detectors. If the photon number state projected to the Da1 and Da2 detectors is $|s_1\rangle|s_2\rangle$, the projecting probability $P_{E_i|s_1s_2}$ corresponding to event E_i (i = 1, 2, 3, 4) can be obtained as shown in Table 2.

Table 2. Probability of the E_i (i = 1, 2, 3, 4) event occurring.

Case	$P_{E_1\|s_1s_2}$	$P_{E_2\|s_1s_2}$	$P_{E_3\|s_1s_2}$	$P_{E_4\|s_1s_2}$
$s_1 = 0, s_2 = 0$	$(1-d_1)(1-d_2)$	$d_1(1-d_2)$	$(1-d_1)d_2$	d_1d_2
$s_1 \neq 0, s_2 = 0$	0	$(1-d_2)$	0	d_2
$s_1 = 0, s_2 \neq 0$	0	0	$(1-d_1)$	d_1
$s_1 \neq 0, s_2 \neq 0$	0	0	0	1

For any n-photon state, the projecting probability $P_{s_1s_2|n}$ projecting into state $|s_1\rangle|s_2\rangle$ can be written as

$$\begin{aligned} P_{s_1s_2|n} &= \sum_{k=0}^{n}\sum_{s_2=0}^{n-k}\sum_{s_1=0}^{k} C_n^k t^k (1-t)^{n-k} C_k^{s_1} \eta_1^{s_1} (1-\eta_1)^{k-s_1} C_{n-k}^{s_2} \eta_2^{s_2} (1-\eta_2)^{n-k-s_2} \\ &= \sum_{k=0}^{n}\sum_{s_2=0}^{n-k}\sum_{s_1=0}^{k} \frac{n! t^k (1-t)^{n-k} \eta_1^{s_1} \eta_2^{s_2} (1-\eta_1)^{k-s_1} (1-\eta_2)^{n-k-s_2}}{s_1! s_2! (k-s_1)! (n-k-s_2)!}, \end{aligned} \tag{2}$$

where t represents the transmittance of BS, and η_1 and η_2 represent the detection efficiency of detector Da1 and detector Da2, respectively.

Therefore, for any n-photon state, the probability of obtaining E_i event can be written as

$$P_{E_i|n} = \sum_{s_1s_2} P_{E_i|s_1s_2} P_{s_1s_2|n}. \tag{3}$$

Then, we can obtain the probability distribution of detection events $P_n^{E_1}$ as

$$P_n^{E_i} = P_n \sum_{s_1s_2} P_{E_i|s_1s_2} P_{s_1s_2|n} \tag{4}$$

where P_n is the photon-number distribution of the PDC process and it can be either a thermal or Poisson distribution, as introduced in [48,49].

4.2. The Parameter Estimation

As shown in Table 3, we take E_1 as the signal window event and other events as the decoy window events. According to Ref. [15], we can obtain the key rate of our protocol as

$$R = 2\epsilon(1-\epsilon) P_1^{E_1E_1} Y_1 [1 - H_2(e_1)] - Q_{E_1E_1} f H_2(E_{E_1E_1}), \tag{5}$$

where $P_1^{E_1E_1}$ is the probability distribution of single-photon states in the signal window, i.e., $P_n^{E_1E_1} = \sum_{k=0}^{n} P_k^{E_1} P_{n-k}^{E_1}$ [27]. f is the error correction inefficiency; $H_2(a) = -x \log_2 a - (1-a)\log_2(1-a)$; Y_1 and e_1 are the yield and error rate of single-photon states. $Q_{E_1E_1}$ and $E_{E_1E_1}$ are the total gain and error rate of signal states in the signal window, respectively.

Table 3. Definition of signal window and decoy window based on the detection events.

Sender	Signal Window	Decoy Windows
Alice	E_1	other events
Bob	E_1	other events

In the decoy window, we still use the WCPs and two weaks + vacuum decoy-state method as the original SNS protocol. According to the previous decoy-state method [7,15,24,27,32,33], we can obtain the lower bound of Y_1 and the upper bound of e_1 as follows:

$$Y_1 \geq \frac{P_2^{\mu}(Q_v - P_0^v Y_0) - P_2^v (Q_{\mu} - P_0^{\mu} Y_0)}{P_2^{\mu} P_1^v - P_2^v P_1^{\mu}}, \tag{6}$$

$$e_1 \leq \frac{Q_v E_v - P_0^v Y_0 e_0}{P_0^v Y_1}, \tag{7}$$

where the subscript 0 indicates that Alice and Bob prepare a vacuum state. P_n^{μ} (n = 0, 1, 2) is the probability distribution of intensity μ, and the total photon number is n. Q_{μ} (Q_v) and E_{μ} (E_v) are the gain and quantum bit error rate (QBER) of intensity μ (v).

5. Numerical Simulations

In this part, we present some results of the numerical simulation. Here, we focus on the symmetric case, which means that the device parameters at the Alice side and Bob side are identical. To simplify the calculation, we also let $d_1 = d_2 = d_L$ and $\eta_1 = \eta_2 = \eta_L$. According to Equation (4), we can obtain the simplified probability distribution $P_n^{E_1}$ for the Alice side and Bob side as

$$P_n^{E_1} = C_\mu (1-d_L)^2 (1-\eta_L)^n P_n, \tag{8}$$

where P_n is a Poissonian distribution, i.e., $P_n = \frac{u^n}{n!} e^{-u}$. Here, C_μ is the normalization factor, which is $C_\mu^{-1} = \sum_{n=0}^{\infty} P_n^{E_1}$.

Next, we derive the values that should be observed in the experiment. According to Refs. [24,26], the corresponding gains and the QBERs in the signal window are given by

$$\begin{aligned} Q_{E_1E_1} = {} & (1-\epsilon)^2 Y_0 + 4\epsilon(1-\epsilon)(1-d_c) \sum_n P_n^{E_1} (1-\eta)^n \sum_n P_n^{E_1} (1-(1-d_c)(1-\eta)^n) \\ & + 2\epsilon^2 (1-d_c) \sum_n P_n^{E_1E_1} (1-\eta)^n \sum_n P_n^{E_1E_1} (1-(1-d_c)(1-\eta)^n), \end{aligned} \tag{9}$$

$$E_{E_1E_1} Q_{E_1E_1} = (1-\epsilon)^2 Y_0 + 2\epsilon^2 (1-d_c) \sum_n P_n^{E_1E_1} (1-\eta)^n \sum_n P_n^{E_1E_s} (1-(1-d_c)(1-\eta)^n), \tag{10}$$

where Y_0 is the yield of the vacuum pulse; d_c is the dark count rate of detectors at the Charlie side; η is the total system efficiency, which is $\eta = \eta_d \eta_c$; η_d is the detection efficiency in Charlie's part; η_c is the transmittance of the quantum channel, $\eta_c = 10^{-\frac{\alpha l}{10}}$, α is the fiber loss coefficient and l is the distance between Alice and Bob. The device parameters used in numerical simulations are listed in Table 4.

Table 4. Device parameters used in numerical simulations.

α	e_0	η_d	η_L	d_c	d_L	f
0.2	0.5	0.5	0.5	10^{-10}	10^{-10}	1.10

Figure 2 shows the comparison of the key rates between the passive decoy-state SNS-QKD and the original SNS-QKD. Note that the performance of our scheme is also related to the quality of local detectors, e.g., the dark count rate and the detection efficiency. The simulation results indicate that, with the passive decoy-state scheme, our protocol can have a performance that is close to that of the original SNS protocol. Moreover, they all exceed the PLOB limit when $l \geq 300$ km.

Figure 3 shows the performance of both the original SNS protocol and passive decoy-state SNS-QKD simulated under misalignment errors e_a. The misalignment error rates are set as 0.015, 0.15 and 0.30, respectively. Moreover, we also add an MDI-QKD curve for comparison. For the key rate of MDI-QKD, the misalignment error rate of X-basis is set to 0.015 and Z-basis is set to 0. The numerical results show that passive decoy-state SNS-QKD still performs well under different misalignment errors, as its performance remains close to the original SNS protocol. In addition, compared with the MDI-QKD, our protocol has better key rate performance, even if the misalignment error is as high as 0.25. In other words, the proposed protocol can still tolerate quite high misalignment errors.

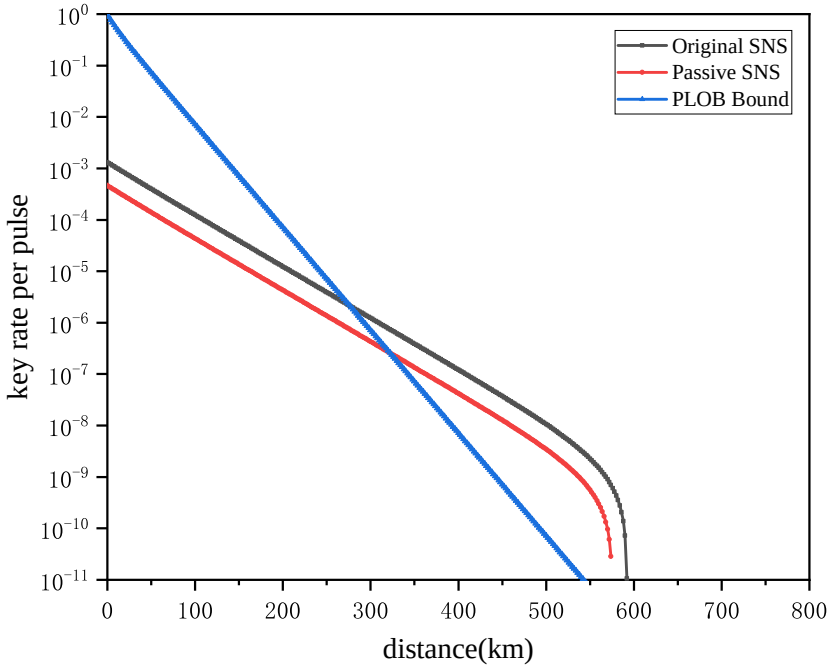

Figure 2. The performance of the passive decoy-state SNS-QKD compared to original SNS protocol.

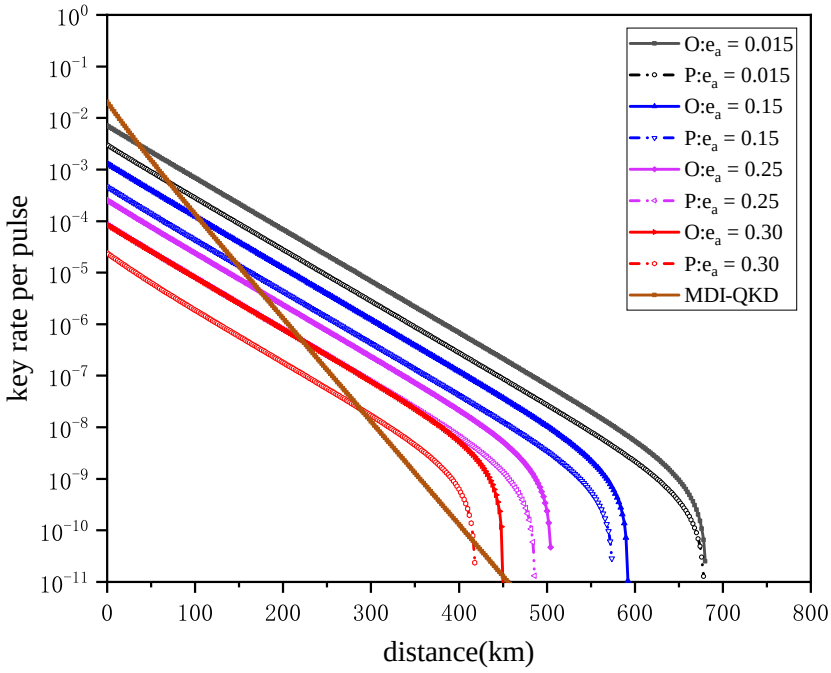

Figure 3. The performance of both original SNS protocol and passive decoy-state SNS-QKD is simulated under misalignment errors e_a. P: Passive decoy-state SNS-QKD. O: Original SNS-QKD. MDI-QKD: MDI-QKD with active decoy-state method in coherent states.

Figure 4 shows the comparison of the tolerance of passive decoy SNS-QKD and original SNS-QKD to misalignment errors e_a. The simulation distance is set to 300 km. Obviously, the SNS-QKD with the passive decoy-state scheme is very close to the original SNS-QKD protocol. Even if the misalignment error reaches 0.30, the performance of the two protocols is still good. This shows that the proposed protocol still retains the advantages of the original SNS-QKD protocol, indicating that the SNS protocol has a broader prospect in implementing long-distance QKD.

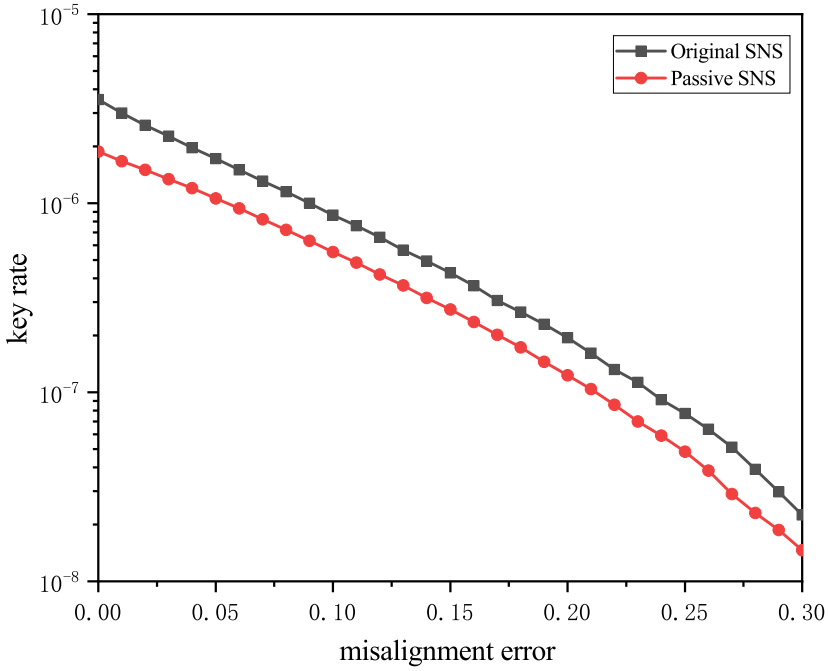

Figure 4. Key rates as a function of the misalignment error when the distance between Alice and Bob is 300 km.

6. Conclusions

In summary, we have proposed the passive decoy-state SNS-QKD protocol to enhance the security of the source of the SNS-QKD protocol. We have presented the framework of the passive decoy-state SNS-QKD protocol and have analyzed the security of the proposed protocol. The numerical simulation results have demonstrated that the key rates of our proposed protocol are close to the original SNS-QKD, which uses the active decoy-state method. Moreover, our protocol can tolerate larger misalignment errors in QKD systems, indicating that the SNS protocol can still have a long transmission distance with a passive decoy-state in real-life QKD systems. Therefore, our protocol represents a further step toward the application of the SNS-QKD.

Author Contributions: Conceptualization, K.X. and Z.S.; investigation, K.X.; writing—review and editing, K.X., S.Z., Z.S. and Q.M.; funding acquisition, Z.S. 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 (61871234) and the open research fund of the Key Lab of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry of Education (JZNY202104).

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. Lo, H.K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, *283*, 2050–2056. [CrossRef] [PubMed]
2. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441. [CrossRef] [PubMed]
3. Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **2001**, *48*, 351–406. [CrossRef]

4. Bennett, C.H.; 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. C175–C179.
5. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef] [PubMed]
6. Ma, X.; Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **2012**, *86*, 062319. [CrossRef]
7. Wang, X.B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Phys. Rev. A* **2013**, *87*, 012320. [CrossRef]
8. Zhou, Y.H.; Yu, Z.W.; Wang, X.B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys. Rev. A* **2016**, *93*, 042324. [CrossRef]
9. Li, Z.; Zhang, Y.C.; Xu, F.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 052301. [CrossRef]
10. Sasaki, T.; Yamamoto, Y.; Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **2014**, *509*, 475–478. [CrossRef]
11. Wang, L.; Zhao, S. Round-robin diferential-phase-shift quantum key distribution with heralded pair-coherent sources. *Quantum Inf. Process.* **2017**, *16*, 100. [CrossRef]
12. Mao, Q.P.; Wang, L.; Zhao, S.M. Plug-and-play round-robin differential phase-shift quantum key distribution. *Sci. Rep.* **2017**, *7*, 1–8.
13. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 1–15. [CrossRef] [PubMed]
14. 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] [PubMed]
15. 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]
16. Xu, H.; Yu, Z.W.; Jiang, C.; Hu, X.L.; Wang, X.B. Sending-or-not-sending twin-field quantum key distribution: Breaking the direct transmission key rate. *Phys. Rev. A* **2020**, *101*, 042330. [CrossRef]
17. Ma, X.; Zeng, P.; Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X* **2018**, *8*, 031043. [CrossRef]
18. Chen, G.; Wang, L.; Li, W.; Zhao, Y.; Zhao, S.M.; Gruska, J. Multiple-pulse phase-matching quantum key distribution. *Quantum Inf. Process.* **2020**, *19*, 1–16. [CrossRef]
19. Yu, Y.; Wang, L.; Zhao, S.; Mao, Q. Decoy-state phase-matching quantum key distribution with source errors. *Opt. Express* **2021**, *29*, 2227–2243. [CrossRef]
20. Yu, B.; Mao, Q.; Zhu, X.; Yu, Y.; Zhao, S. Phase-matching quantum key distribution based on pulse-position modulation. *Phys. Lett. A* **2021**, *418*, 127702. [CrossRef]
21. Lin, J.; Ltkenhaus, N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* **2018**, *98*, 042332. [CrossRef]
22. 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]
23. Hu, X.L.; Jiang, C.; Yu, Z.W.; Wang, X.B. Sending-or-not-sending twin-field protocol for quantum key distribution with asymmetric source parameters. *Phys. Rev. A* **2019**, *100*, 062337. [CrossRef]
24. Yu, Z.W.; Hu, X.L.; Jiang, C.; Xu, H.; Wang, X.B. Sending-or-not-sending twin-field quantum key distribution in practice. *Sci. Rep.* **2019**, *9*, 1–8. [CrossRef] [PubMed]
25. Jiang, C.; Yu, Z.W.; Hu, X.L.; Wang, X.B. Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses. *Phys. Rev. Appl.* **2019**, *12*, 024061. [CrossRef]
26. Zhang, C.H.; Zhang, C.M.; Wang, Q. Twin-field quantum key distribution with modified coherent states. *Opt. Lett.* **2019**, *44*, 1468–1471. [CrossRef]
27. Qiao, Y.; Chen, Z.; Zhang, Y.; Xu, B.; Guo, H. Sending-or-Not-Sending Twin-Field Quantum Key Distribution with Light Source Monitoring. *Entropy* **2020**, *22*, 36. [CrossRef]
28. Xue, K.; Zhao, S.; Mao, Q.; Xu, R. Plug-and-play sending-or-not-sending twin-field quantum key distribution. *Quantum Inf. Process.* **2021**, *20*, 1–16. [CrossRef]
29. 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]
30. Xu, H.; Hu, X.L.; Feng, X.L.; Wang, X.B. Hybrid protocol for sending-or-not-sending twin-field quantum key distribution. *Opt. Lett.* **2020**, *45*, 4120–4123. [CrossRef]
31. Hwang, W.Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef]
32. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 012326. [CrossRef]
33. Lo, H.K.; Ma, X.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef] [PubMed]
34. Wang, X.B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef] [PubMed]

35. Wang, X.B. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Phys. Rev. A* **2005**, *72*, 012322. [CrossRef]
36. Zhao, Y.; Qi, B.; Lo, H.K.; Qian, L. Security analysis of an untrusted source for quantum key distribution: Passive approach. *New J. Phys.* **2010**, *12*, 023024. [CrossRef]
37. Tang, G.Z.; Sun, S.H.; Xu, F.; Chen, H.; Li, C.Y.; Liang, L.M. Experimental asymmetric plug-and-play measurement-device-independent quantum key distribution. *Phys. Rev. A* **2016**, *94*, 032326. [CrossRef]
38. Jiang, M.S.; Sun, S.H.; Li, C.Y.; Liang, L.M. Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states. *Phys. Rev. A* **2012**, *86*, 032310. [CrossRef]
39. Mauerer, W.; Silberhorn, C. Quantum key distribution with passive decoy state selection. *Phys. Rev. A* **2007**, *75*, 050305. [CrossRef]
40. Adachi, Y.; Yamamoto, T.; Koashi, M.; Imoto, N. Simple and efficient quantum key distribution with parametric down-conversion. *Phys. Rev. Lett.* **2007**, *99*, 180503. [CrossRef]
41. Wang, Q.; Zhang, C.H.; Wang, X.B. Scheme for realizing passive quantum key distribution with heralded single-photon sources. *Phys. Rev. A* **2016**, *93*, 032312. [CrossRef]
42. Zhang, C.H.; Zhang, C.M.; Wang, Q. Efficient passive measurement-device-independent quantum key distribution. *Phys. Rev. A* **2019**, *99*, 052325. [CrossRef]
43. Teng, J.; Lu, F.-Y.; Yin, Z.-Q.; Fan-Yuan, G.-J.; Wang, R.; Wang, S.; Chen, W.; Huang, W.; Xu, B.-J.; Guo, G.-C.; et al. Twin-field quantum key distribution with passive-decoy state. *New J. Phys.* **2020**, *22*, 103017. [CrossRef]
44. Zhang, C.-H.; Wang, D.; Zhou, X.-Y.; Wang, S.; Zhang, L.-B.; Yin, Z.-Q.; Chen, W.; Han, Z.-F.; Guo, G.-C.; Wang, Q. Proof-of-principle demonstration of parametric down-conversion source-based quantum key distribution over 40 dB channel loss. *Opt. Express* **2018**, *26*, 25921–25933. [CrossRef] [PubMed]
45. Yurke, B.; Potasek, M. Obtainment of thermal noise from a pure quantum state. *Phys. Rev. A* **1987**, *36*, 3464. [CrossRef]
46. Barreiro, J.T.; Langford, N.K.; Peters, N.A.; Kwiat, P.G. Generation of hyperentangled photon pairs. *Phys. Rev. Lett.* **2005**, *95*, 260501. [CrossRef]
47. Li, X.; Voss, P.L.; Sharping, J.E.; Kumar, P. Optical-fiber source of polarization-entangled photons in the 1550 nm telecom band. *Phys. Rev. Lett.* **2005**, *94*, 053601. [CrossRef]
48. Ribordy, G.; Brendel, J.; Gautier, J.D.; Gisin, N.; Zbinden, H. Long-distance entanglement-based quantum key distribution. *Phys. Rev. A* **2000**, *63*, 012309. [CrossRef]
49. Mori, S.; Söderholm, J.; Namekata, N.; Inoue, S. On the distribution of 1550-nm photon pairs efficiently generated using a periodically poled lithium niobate waveguide. *Opt. Commun.* **2006**, *264*, 156–162. [CrossRef]