entropy

MDPI

Article

Sending-or-Not-Sending Twin-Field Quantum Key Distribution with Light Source Monitoring

Yucheng Qiao [1], Ziyang Chen [1], Yichen Zhang [2], Bingjie Xu [3] and Hong Guo [1,*]

[1] State Key Laboratory of Advanced Optical Communication, Systems and Networks, Department of Electronics, and Center for Quantum Information Technology, Peking University, Beijing 100871, China; glqyc251@pku.edu.cn (Y.Q.); chenziyang@pku.edu.cn (Z.C.)

[2] State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China; zhangyc@bupt.edu.cn

[3] Science and Technology on Security Communication Laboratory, Institute of Southwestern Communication, Chengdu 610041, China; xbjpku@163.com

* Correspondence: hongguo@pku.edu.cn

Received: 13 December 2019; Accepted: 25 December 2019; Published: 26 December 2019

Abstract: Twin-field quantum key distribution (TF-QKD) is proposed to achieve a remote key distribution with a maximum secure transmission distance up to over 500 km. Although the security of TF-QKD in its detection part is guaranteed, there are some remaining problems in the source part. The sending-or-not-sending (SNS) protocol is proposed to solve the security problem in the phase post-selection process; however, the light source is still assumed to be an ideal coherent state. This assumption is not satisfied in real-life QKD systems, leading to practical secure issues. In this paper, we discuss the condition that the photon number distribution (PND) of the source is unknown for the SNS protocol, demonstrate that the security analysis is still valid under a source with unknown PND, and show that with light source monitoring, the performance of the SNS protocol can remain almost unchanged.

Keywords: quantum key distribution; twin-fields; sending-or-not-sending; light source monitoring

1. Introduction

Quantum key distribution (QKD) provides a way for different communication parties to share a set of identical security keys [1,2]. The security of QKD is based on the laws of quantum physics and has been proved theoretically in different ways in the past decades. In addition to security analysis, people have also started to study the performance of QKD and to further improve the performance of real-life QKD systems by proposing new protocols [3–7].

Among all proposed protocols, measurement-device-independent (MDI) protocol is meaningful, since it can make up all the security loopholes in the detection part of QKD systems [8]. MDI protocol has developed rapidly in recent years, with many achievements obtained [9–19]. In theory, the application of the decoy state method [20] has been further studied, and more optimized parameter estimation results are obtained to achieve a better performance [9–11]. Besides, different MDI experiment schemes have been proposed [12] and several meaningful experiment achievements, including the field test [13] and the network experiment [14] based on the MDI protocol, have been carried out. Meanwhile, the continuous-variable MDI protocol has also been developed [16–19]. With the developing of experimental research, the MDI protocol achieved a transmission distance of 404 km in 2016, which was the farthest distance for standard QKD at that time [15].

The transmission distance of QKD has been further increased recently. Based on the MDI protocol, an extraordinary protocol called twin-field quantum key distribution (TF-QKD) was proposed by

Lucamarini et al. in 2018, which can increase the transmission distance to over 550 km on standard optical fibers without quantum repeaters [21]. Because of its outstanding advantage in transmission distance, TF-QKD has recently been the subject of a lot of follow-up research [22–29]. Actually, in the original protocol, the phase randomization process will lead to secure issues since the information of random phase is announced to Eve in the post-selection process [30]. In further research, different types of modified TF-QKD protocols have been proposed to improve the incomplete security analysis [22–26]. Through classifying the signals [22], or adding an extra test mode [23], or using a pre-selected global phase [25,26], the security loophole of the post-selected part can be resolved. With the modified protocols, long-distance TF-QKD experiments have already been implemented [28,29]. Recently, an exciting experimental work has shown that the transmission distance for TF-QKD can reach over 500 km in practice [28], showing that TF-type protocols can significantly improve the transmission distance with the currently available technology.

Among those TF-type protocols, the sending-or-not-sending (SNS) protocol proposed by Wang et al. is an effective scheme to combine with the decoy state method to solve the phase randomization problem. In the SNS protocol, there is no post-selection process for the random phases of the signal bits, which are used to generate the final secret keys, thus the problem is avoided [22]. By optimizing the proportion of the sending and not-sending signals, the SNS protocol can still achieve a very long transmission distance.

A remaining problem with the SNS protocol is that the prepared quantum state in the source is assumed to be an ideal coherent state. Actually, the assumption could be broken since the prepared state will deviate from the ideal coherent state due to the non-ideality of the practical laser [31]. Moreover, since the light source structure in the SNS protocol is similar to the BB84 protocol, there will also be an untrusted source problem [32–36] in the source part, causing the photon number distribution (PND) of the light source to be unknown, and the prepared state to no longer be a coherent state.

In this paper, we provide further discussion of the SNS protocol under the unknown PND condition (UPC). By analyzing the form of the prepared state in Eve's view, it is shown that the security analysis in the SNS protocol is still valid without the coherent state assumption, and the final secret key rate can be derived naturally. By applying a light source monitoring (LSM) method proposed previously [37,38], all relevant parameters can be estimated compactly, thus the secret key rate of the SNS protocol under UPC can be obtained. Moreover, it is indicated that the performance of the SNS protocol under UPC can almost keep the same ideal source condition through the numerical simulation.

The paper is organized as follows. In Section 2, we first analyze the security of the SNS protocol under UPC and give the calculation method of the secret key rate for the SNS protocol under UPC, then introduce an LSM method to obtain tight bounds of the parameters needed in calculating the secret key rate. In Section 3, we show the simulation results by applying the LSM method in the SNS protocol under UPC. Finally, we provide conclusion to our work in Section 4.

2. SNS Protocol with LSM

2.1. Security Analysis under UPC

In the SNS protocol [22,27], Alice (Bob) prepares a coherent state with an intensity μ_A (μ_B), a random modulated phase δ_A (δ_B) and a global phase γ_A (γ_B). Only the states where Alice and Bob choose the same intensity ($\mu_A = \mu_B = \mu$) will be retained for discussion, thus the joint state sent by Alice and Bob is $|\sqrt{\mu}e^{i(\delta_A+\gamma_A)}\rangle|\sqrt{\mu}e^{i(\delta_B+\gamma_B)}\rangle$. In Eve's view, it has the convex form

$$\rho_{AB} = \sum_k p_k(\mu)|\psi_k\rangle\langle\psi_k|, \tag{1}$$

where $|\psi_k\rangle$ refers to a joint state with total photon numbers k, and $p_k(\mu)$ refers to the probability that the joint state contains k photons totally [22]. Specifically, the single-photon part of the state has the form of

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[e^{i(\delta_B+\gamma_B)}|0\rangle_A|1\rangle_B + e^{i(\delta_A+\gamma_A)}|1\rangle_A|0\rangle_B]. \tag{2}$$

$|\psi_1\rangle$ plays an important role during the whole security analysis of the SNS protocol [22]. In fact, the equivalent virtual protocols discussed in the security analysis focus on the single-photon part and the security analysis could remain valid when the phase difference between the two parts of the single state $|1\rangle_A|0\rangle_B$ and $|0\rangle_A|1\rangle_B$ remains to be

$$\Delta\phi = \delta_A + \gamma_A - \delta_B - \gamma_B. \tag{3}$$

Under UPC, the quantum state prepared by Alice (Bob) is no longer an ideal coherent state $|\sqrt{\mu}e^{i(\delta_A+\gamma_A)}\rangle$ ($|\sqrt{\mu}e^{i(\delta_B+\gamma_B)}\rangle$), but a state with arbitrary PND, which can be written as $|\psi_A\rangle = \sum_k e^{ik(\delta_A+\gamma_A)}\sqrt{P_{k,A}(\mu)}|k\rangle_A$ ($|\psi_B\rangle = \sum_k e^{ik(\delta_B+\gamma_B)}\sqrt{P_{k,B}(\mu)}|k\rangle_B$) after the modulation process, where $P_{k,A}(\mu)$ ($P_{k,B}(\mu)$) is completely unknown.

As a result, with the analysis shown in Appendix A, the joint state sent by Alice and Bob can still have the convex form

$$\rho_{AB} = \sum_n p_n(\mu)|\psi'_n\rangle\langle\psi'_n| \tag{4}$$

in Eve's view, with the n-photon state

$$|\psi'_n\rangle = \frac{1}{\sqrt{p_n(\mu)}}\sum_{k=0}^{n}\sqrt{P_{k,A}(\mu)P_{n-k,B}(\mu)}e^{ik\Delta\phi}|k\rangle_A|n-k\rangle_B, \tag{5}$$

and the probability of n-photon

$$p_n(\mu) = \sum_{k=0}^{n} P_{k,A}(\mu)P_{n-k,B}(\mu). \tag{6}$$

Specifically, the single photon part of ρ_{AB} under UPC can be written as

$$|\psi'_1\rangle = \frac{1}{\sqrt{2}}[|0\rangle_A|1\rangle_B + e^{i\Delta\phi}|1\rangle_A|0\rangle_B] \tag{7}$$

with a symmetric condition

$$P_{k,A}(\mu) = P_{k,B}(\mu) = P_k(\mu), \tag{8}$$

which is also assumed in the original SNS protocol [22]. This result indicates that the original security analysis can be directly applied to UPC, since the phase difference between $|1\rangle_A|0\rangle_B$ and $|0\rangle_A|1\rangle_B$ is still $\Delta\phi$, that is, $|\psi'_1\rangle$ only has a global phase difference with $|\psi_1\rangle$ in Equation (2).

Secret Key Rate

Unlike the original TF-QKD, the SNS protocol divides all the transmitted light pulses into two categories, which are called signal windows and decoy windows [20,22]. In the signal window (equivalent to Z-basis), Alice (Bob) randomly chooses to send or not send a signal pulse, and the data are used to generate keys. In the decoy window (equivalent to X-basis), Alice (Bob) sends decoy states with different intensities and the data are used to estimate the count rate and phase error rate of the signals' single photon part. In addition, there is a post-selection process for the random phases δ_A, δ_B to ensure more accurate estimation results, which originates from TF-QKD.

The secret key rate of the SNS protocol has been given as [22,27]:

$$R = 2\epsilon(1-\epsilon)P_1^L(\mu_s)s_1^L[1 - H(e_1^{ph,U})] - fS_Z H(E_Z), \tag{9}$$

in which ϵ is the probability that Alice (Bob) chooses to send out a signal pulse (it can be preset in the protocol), $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function, $P_1^L(\mu_s)$ is the

lower bound of the probability that a state with intensity μ_s sent in signal windows contains single photon, s_1^L and e_1^U refer to the lower bound of the count rate and the upper bound of phase error rate for the single photon part of signals, S_Z and E_Z refer to the count rate and the bit error rate of the signals. In decoy windows, a three-intensity decoy method with intensities $\mu_{d_0} = 0, \mu_{d_1}, \mu_{d_2}$ and $\mu_{d_2} > \mu_{d_1} > 0$ is used to estimate s_1^L and e_1^U and the results are obtained as [22]

$$s_1^L = \frac{p_2(\mu_{d_2})[S_{\mu_{d_1}} - p_0(\mu_{d_1})S_0] - p_2(\mu_{d_1})[S_{\mu_{d_2}} - p_0(\mu_{d_2})S_0]}{p_2(\mu_{d_2})p_1(\mu_{d_1}) - p_2(\mu_{d_1})p_1(\mu_{d_2})}, \tag{10}$$

$$e_1^{ph,U} = \frac{S_{\mu_{d_1}} E_{\mu_{d_1}} - p_0(\mu_{d_1})S_0/2}{p_1(\mu_{d_1})s_1^L}, \tag{11}$$

where $p_0(\mu_{d_k}), p_1(\mu_{d_k}), p_2(\mu_{d_k})$ $(k = 0, 1, 2)$ are the probabilities that a state with intensity μ_{d_k} sent in decoy windows contains zero, single or two photons, $S_{\mu_{d_k}}, E_{\mu_{d_k}}$ are the count rate and bit error rate of a state with intensity μ_{d_k} sent in decoy windows.

In the original SNS protocol, the light source is assumed to be able to prepare ideal coherent states [22], thus the PND of the light source satisfies Poisson distribution for each of Alice and Bob, that is,

$$P_{n,A}(\mu) = P_{n,B}(\mu) = P_n(\mu) = e^{-\mu}\frac{\mu^n}{n!} \tag{12}$$

for $\mu = \{\mu_s, \mu_{d_1}, \mu_{d_2}\}$, hence the probabilities $p_n(\mu)$ $(n = 0, 1, 2)$ obtained in Equation (6) can be directly calculated as:

$$\begin{aligned} &p_0(\mu) = P_0^2(\mu), p_1(\mu) = 2P_0(\mu)P_1(\mu), \\ &p_2(\mu) = 2P_0(\mu)P_2(\mu) + P_1^2(\mu). \end{aligned} \tag{13}$$

When $p_n(\mu)$ are known, the parameters s_1^L and e_1^U in Equations (10) and (11) can be estimated. In addition, the probability $P_1^L(\mu_s)$ is also obtained exactly from Equation (12). With these results, the secret key rate in Equation (9) can eventually be calculated.

However, as mentioned above, the probabilities $p_n(\mu)$ become unknown under UPC, though the security analysis can be held. Fortunately, as analyzed in Reference [39], the decoy-state method is still valid under UPC when the lower and upper bounds of $p_n(\mu)$ $(n = 0, 1, 2)$ are obtained, and the results of s_1^L and e_1^U can be rewritten as

$$s_1^L = \frac{p_2^L(\mu_{d_2})[S_{\mu_{d_1}} - p_0^U(\mu_{d_1})S_0] - p_2^U(\mu_{d_1})[S_{\mu_{d_2}} - p_0^L(\mu_{d_2})S_0]}{p_2^U(\mu_{d_2})p_1^U(\mu_{d_1}) - p_2^L(\mu_{d_1})p_1^L(\mu_{d_2})}, \tag{14}$$

$$e_1^{ph,U} = \frac{S_{\mu_{d_1}} E_{\mu_{d_1}} - p_0^L(\mu_{d_1})S_0/2}{p_1^L(\mu_{d_1})s_1^L}, \tag{15}$$

where $p_n^{L(U)}(\mu)$ refers to the lower (upper) bound of $p_n(\mu)$. With Equation (6) , $p_n^{L(U)}(\mu)$ $(n = 0, 1, 2)$ can be obtained as

$$\begin{aligned} &p_0^{L(U)}(\mu) = [P_0^{L(U)}(\mu)]^2, p_1^{L(U)}(\mu) = 2P_0^{L(U)}(\mu)P_1^{L(U)}(\mu), \\ &p_2^{L(U)}(\mu) = 2P_0^{L(U)}(\mu)P_2^{L(U)}(\mu) + [P_1^{L(U)}(\mu)]^2 \end{aligned} \tag{16}$$

with Equation (8), hence the secret key rate can still be calculated effectively if tight bounds of $P_n(\mu)$ are obtained.

2.2. Parameters Estimation with LSM

The source structure in the SNS protocol is similar to that of the BB84 and MDI protocol, therefore it is possible to apply the LSM scheme proposed in the BB84 and MDI protocol to the SNS protocol to

estimate $P_n(\mu)$. Recently, a new LSM scheme proposed by us in the MDI protocol gives tight bounds of $P_n(\mu)$ in each of Alice's and Bob's part under UPC [38]. Since the SNS protocol and the MDI protocol have the same structure in the intensity modulation part, the same LSM module can be added to the SNS protocol as shown in Figure 1, and with the extra LSM module, the same results can be obtained in the SNS protocol as follows [38]:

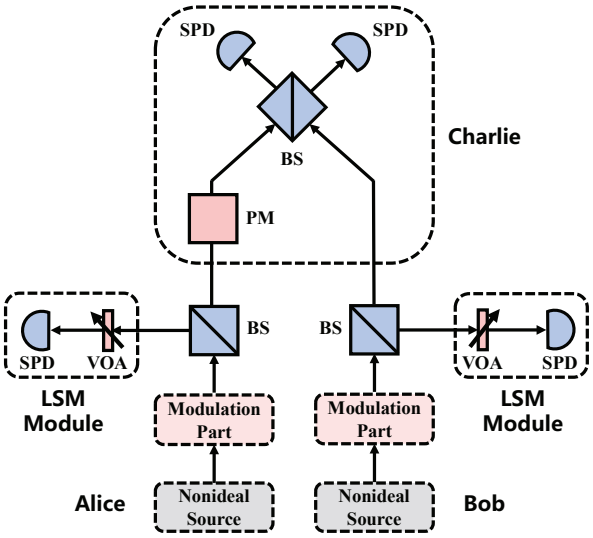

Figure 1. The structure of the sending-or-not-sending (SNS) protocol with an extra LSM module in each of Alice's and Bob's parts. The LSM module is made up of a variable optical attenuators (VOA) and a single photon detector (SPD). By changing the attenuation coefficient of the VOA, various sets of the results on the responding probability of the SPD are obtained, which can be used to estimate $P_n(\mu)$ effectively. The details of the monitoring scheme have been discussed in Reference [38].

$$P_0^U(\mu) = P_0^L(\mu) = \frac{P^\mu(\eta_0)}{1 - Y_0}, \tag{17}$$

$$P_1^L(\mu) = \frac{(1-\eta_2)^2 P^\mu(\eta_1) - (1-\eta_1)^2 P^\mu(\eta_2)}{(1-Y_0)(1-\eta_1)(1-\eta_2)(\eta_1-\eta_2)} - (\frac{1}{1-\eta_1} + \frac{1}{1-\eta_2}) P_0^U(\mu), \tag{18}$$

$$\begin{aligned} P_1^U(\mu) = {} & \frac{(1-\eta_2)(1-\eta_1)}{[1-\eta_2-(1-\eta_1)(2-\eta_1)]} \{ \frac{P^\mu(\eta_1)}{(1-\eta_1)^2(1-Y_0)} + \frac{[1-(1-\eta_2)^3]}{\eta_2(1-\eta_2)^2} P_0^U(\mu) \\ & + \frac{1-\eta_2}{\eta_2} - \frac{P^\mu(\eta_2)}{\eta_2(1-\eta_2)^2(1-Y_0)} - \frac{P_0^L(\mu)}{(1-\eta_1)^2} \}, \end{aligned} \tag{19}$$

$$P_2^L(\mu) = \frac{P^\mu(\eta_2)}{(1-Y_0)(1-\eta_2)^2\eta_2} - \frac{1-\eta_2}{\eta_2} - \frac{[1-(1-\eta_2)^3]}{(1-\eta_2)^2\eta_2} P_0^U(\mu) - \frac{2-\eta_2}{1-\eta_2} P_1^U(\mu), \tag{20}$$

$$P_2^U(\mu) = \frac{P^\mu(\eta_2)}{(1-Y_0)(1-\eta_2)^2} - \frac{P_0^L(\mu)}{(1-\eta_2)^2} - \frac{P_1^L(\mu)}{1-\eta_2} \tag{21}$$

with a condition

$$\eta_1(2-\eta_2) > 1, \tag{22}$$

where $\eta_k (k = 0, 1, 2)$ is the variable attenuation coefficient in the extra LSM module, $P^\mu(\eta_k)$ is the probabilities of the single photon detector's (SPD) not responding in the LSM module, and Y_0 is the dark count rate of the SPD. When $P_n(\mu)$ are estimated with the LSM scheme, the key parameters s_1^L, e_1^U in Equations (14) and (15) can be calculated, and the secret key rate of SNS protocol under UPC is obtained.

3. Performance with Numerical Simulation

The performance of the original SNS protocol and the SNS protocol with the LSM scheme can be compared with a determined light source condition. Considering an ideal simulation circumstance

first [22], the PND of the light source, $P_n(\mu)$, is assumed to satisfy Equation (12). In this case, the probabilities $P^{\mu}(\eta)$ in the LSM scheme can be simulated as [38]

$$P^{\mu}(\eta) = (1 - Y_0)e^{-\eta\mu}, \tag{23}$$

and the estimation results of $P_n(\mu)$ can be calculated with Equations (17)–(21). Except $P^{\mu}(\eta)$, other parameters used in Equations (9)–(11), (14) and (15), such as $S_{\mu_{d_k}}, E_{\mu_{d_k}}, S_Z, E_Z$, can be simulated with the same method discussed in the original SNS protocol [22,27], hence the final secret key rate can be calculated.

To compare the performance of the LSM scheme and the original SNS protocol under ideal simulation conditions, the simulation parameters, which are listed in Table 1, are set to be the same as in Reference [22]. Besides, for the LSM scheme, we set the attenuation coefficient as $\eta_0 = 1$, $\eta_1 = 0.95$, $\eta_2 = 0.9$ to obtain tight estimation results of $P_n(\mu)$; other parameters, including the intensities $\mu_s, \mu_{d_1}, \mu_{d_2}$ and the sending probability ϵ, are optimized at different transmission distances for both the original protocol and the SNS protocol with the LSM scheme.

Table 1. Values of parameters used in simulation. α: the fiber loss coefficient (unit: dB/km); Y_0: the dark count rate of the detector; η_D: the detection efficiency; e_{det}: the misalignment error of the QKD system; f: the error correction efficiency.

α	Y_0	η_D	e_{det}	f
0.2	1.0×10^{-11}	80%	1%	1.1

The simulation results shown in Figure 2 indicate that, with the LSM scheme, the SNS protocol under UPC can have a performance that is almost the same as that of the original protocol with an ideal source. Specifically, both cases have a maximum transmission distance of up to over 800 km, and the difference between the LSM scheme and the ideal source condition is only about 0.5 km. Besides, the difference of the secret key rate between them is only about 1% for a typical distance of 100 km.

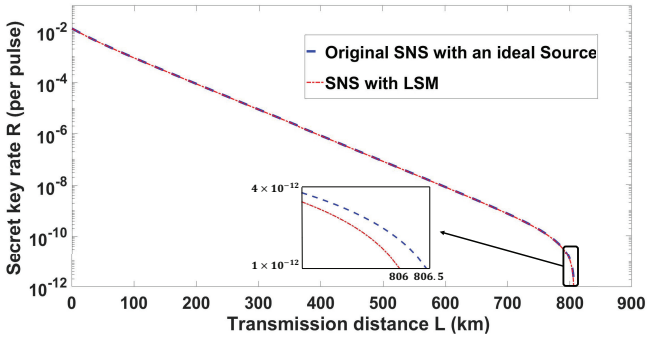

Figure 2. The performance of the proposed LSM scheme (red dash curve) compared to original SNS protocol (blue dash curve) with the parameters set as Table 1. The ratios of secret key rate between the LSM scheme and original SNS protocol are about 99.1%, 98.9%, 98.8% at the distance of 100, 300, 500 km, and the maximum transmission distances of the LSM scheme and original SNS protocol are about 806.0 and 806.5 km.

In order to further analyze the practical performance of the SNS protocol and it with the LSM scheme, it is necessary to consider a more practical simulation circumstance. For a real-life QKD system, the PND of the source's signals is not fixed although without Eve's disturbance [31,40,41]. Under this condition, the performance of the original SNS protocol will be degraded even though the security problem of an unknown PND is ignored. Specifically, the signal sent out from the source can be considered as a fluctuated coherent state with a Gaussian-distributed average photon number μ, which has a probability distribution of

$$P(\mu) = \frac{1}{\sqrt{2\pi}\sigma_\mu} \exp[-\frac{(\mu-\mu_0)^2}{2\sigma_\mu^2}], \tag{24}$$

where μ_0, σ_μ are the mean value and the standard deviation of μ. Without the LSM module, the probabilities $P_n(\mu)$ can only be estimated by assuming that μ belongs to a confidence interval, that is, $\mu \in [\mu_L, \mu_U]$, with a confidence level $\varepsilon = \int_{\mu_L}^{\mu_U} P(\mu)d\mu$, where

$$\mu_L = (1-\delta)\mu_0, \mu_U = (1+\delta)\mu_0, \tag{25}$$

hence the results are

$$\begin{aligned} P_0^{L(U)}(\mu) &= e^{-\mu_{U(L)}}, P_1^{L(U)}(\mu) = \mu_{L(U)} e^{-\mu_{L(U)}}, \\ P_2^{L(U)}(\mu) &= \frac{\mu_{L(U)}^2}{2} e^{-\mu_{L(U)}}. \end{aligned} \tag{26}$$

For the LSM scheme, the probabilities $P^\mu(\eta)$ can be simulated as

$$P^\mu(\eta_i) = (1-Y_0)\exp\left[-\eta_i\mu_0 - \frac{(\eta_i\sigma_\mu)^2}{2}\right] \tag{27}$$

after considering the source fluctuation [36,37], and $P_n(\mu)$ can be estimated by $P^\mu(\eta_i)$ with Equations (17)–(21).

The performance of both the original SNS protocol and the original SNS protocol with LSM are simulated under different fluctuation coefficient $\sigma = \sigma_\mu/\mu_0$. The parameters are changed to be consistent with those in Reference [21] in Table 2 to simulate a more realistic condition, which is close to the practical experimental conditions [28], and $\epsilon, \mu_s, \mu_{d_1}, \mu_{d_2}$ are optimized as well. For the original SNS protocol, the confidence levels are set as $\varepsilon = 1 - 10^{-10}$, and in the LSM scheme, the attenuation coefficients are set as $\eta_0 = 1, \eta_1 = 0.95, \eta_2 = 0.9$. The simulation results under the practical simulation condition shown in Figure 3 indicate that the LSM scheme still performs well in practice, as its performance remains almost the same under the fluctuated light source. As a comparison, the performance of the original SNS protocol decreases obviously with a light source fluctuation $\sigma = 1\%$, and its transmission distance even reduces to less than 500 km when $\sigma = 2\%$. Since the condition $\sigma > 1\%$ is common in real-life QKD systems [40,41], the LSM scheme will have a better performance compared to the original SNS protocol in practice, although only the fluctuation problem is considered.

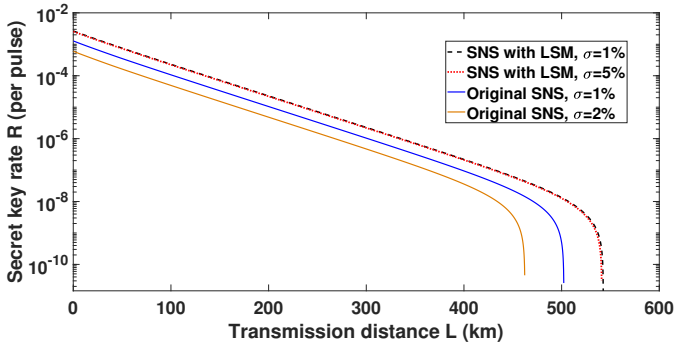

Figure 3. The performance of the LSM scheme with an untrusted and fluctuated light source compared to original SNS protocol. σ: the fluctuation coefficient. For the LSM scheme, we consider a small fluctuation condition $\sigma = 1\%$ (black dash curve) and a large fluctuation condition $\sigma = 5\%$ (red dash curve), and the performance between them is still close. For the original protocol, we consider a small fluctuation condition $\sigma = 1\%$ (blue curve) and a relatively large fluctuation condition $\sigma = 2\%$ (yellow curve), since the condition $\sigma = 2\%$ already has an obviously worse performance than $\sigma = 1\%$.

Table 2. Values of parameters used in simulation (set as in Reference [21] for a more practical condition).

α	Y_0	η_D	e_{det}	f
0.2	1.0×10^{-9}	30%	3%	1.15

4. Conclusions

In summary, we analyze the security of the SNS protocol under UPC, and propose an LSM scheme to solve the unknown PND problem in the source part. An important problem for the SNS protocol is whether its security analysis is still valid without assuming the prepared state is an ideal coherent state. In this paper, we calculate the form of the quantum state sent from Alice and Bob in Eve's view, and show that the single photon part of the state has the same form as the ideal source condition under UPC, thus the security analysis remains valid. We apply the LSM scheme proposed previously to the SNS protocol to estimate the probabilities $p_n(\mu)$ precisely to eventually obtain a tight bound of the secret key rate. Through simulation, we show that, with the proposed LSM scheme, the performance of the SNS protocol under UPC can be almost the same as that of the original SNS protocol with an ideal source. Moreover, the LSM scheme improves the performance of the SNS protocol when considering source fluctuation, indicating that the SNS protocol can still have a long transmission distance with a fluctuated source in real-life QKD systems.

Author Contributions: Conceptualization, Y.Q., Z.C. and Y.Z.; methodology,Y.Q., Z.C. and Y.Z.; validation, Y.Q. and B.X.; formal analysis, Y.Q.; investigation, Y.Q. and Z.C.; resources, Y.Z. and H.G.; writing–original draft preparation, Y.Q.; writing—review and editing, Y.Q., Z.C. and B.X.; visualization, Y.Q.; funding acquisition, H.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Natural Science Foundation of China (Grant Nos. 61531003, 61771439) and the National Science Fund for Distinguished Young Scholars of China (Grant No. 61225003).

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

Appendix A. The Convex Form of ρ_{AB} under UPC

After the modulation of intensity and phase, the quantum state sent by Alice (Bob) can be written as a state with an arbitrary PND, $|\psi_A\rangle = \sum_k e^{ik(\delta_A+\gamma_A)}\sqrt{P_{k,A}(\mu)}|k\rangle_A$ ($|\psi_B\rangle = \sum_k e^{ik(\delta_B+\gamma_B)}\sqrt{P_{k,B}(\mu)}|k\rangle_B$). Although the exact values of $P_{k,A}(\mu), P_{k,B}(\mu)$ are totally unknown, the form of the sent state ρ_{AB} in Eve's view can be calculated because of the randomness of the phase δ_A, δ_B. Actually, similar to the situation of original SNS protocol, the new independent variables $\delta_\pm = \delta_A \pm \delta_B$ can be introduced as well, and the phase δ_+ is completely random for Eve [22], thus in Eve's view, the quantum state sent from Alice and Bob is

$$\begin{aligned}
\rho_{AB} &= \int_0^{2\pi} P(|\psi_A\rangle \otimes |\psi_B\rangle) d\delta_+ \\
&= \int_0^{2\pi} P[\sum_k e^{ik(\delta_A+\gamma_A)}\sqrt{P_{k,A}(\mu)}|k\rangle_A \otimes \sum_m e^{im(\delta_B+\gamma_B)}\sqrt{P_{m,B}(\mu)}|m\rangle_B] d\delta_+ \\
&= \int_0^{2\pi} \sum_k \sum_m P[e^{ik(\delta_A+\gamma_A)}\sqrt{P_{k,A}(\mu)}|k\rangle_A| \otimes e^{im(\delta_B+\gamma_B)}\sqrt{P_{m,B}}(\mu)|m\rangle_B] d\delta_+ \\
&= \sum_k \sum_m \int_0^{2\pi} P[e^{i(\frac{k+m}{2}\delta_+ + \frac{k-m}{2}\delta_- + k\gamma_A + m\gamma_B)}\sqrt{P_{k,A}(\mu)P_{m,B}(\mu)}|k\rangle_A|m\rangle_B] d\delta_+ \\
&= \sum_{k,k',m,m'} \int_0^{2\pi} \sqrt{P_{k,A}(\mu)P_{k',A}(\mu)P_{m,B}(\mu)P_{m',B}(\mu)} e^{i[\frac{k+m-k'-m'}{2}\delta_+ + \frac{k-k'+m'-m}{2}\delta_- + (k-k')\gamma_A + (m-m')\gamma_B]}|k\rangle_A|m\rangle_{BB}\langle m'|_A\langle k'| d\delta_+ \\
&= \sum_{k,k',m,m'} \delta(k+m-k'-m')\sqrt{P_{k,A}(\mu)P_{k',A}(\mu)P_{m,B}(\mu)P_{m',B}(\mu)} e^{i[\frac{k-k'+m'-m}{2}\delta_- + (k-k')\gamma_A + (m-m')\gamma_B]}|k\rangle_A|m\rangle_{BB}\langle m'|_A\langle k'| \\
&= \sum_{k,k',m} \sqrt{P_{k,A}(\mu)P_{k',A}(\mu)P_{m,B}(\mu)P_{k+k'-m,B}(\mu)} e^{i(k-k')\Delta\phi}|k\rangle_A|m\rangle_{BB}\langle k+m-k'|_A\langle k'|,
\end{aligned} \tag{A1}$$

where $P(|x\rangle) = |x\rangle\langle x|$ is the density matrix of $|x\rangle$, $\delta(\cdot)$ is the Dirac delta function, and $\Delta\phi = \delta_A + \gamma_A - \delta_B - \gamma_B$.

The results of Equation (A1) can be written as

$$\rho_{AB} = \sum_n |\psi_n(\mu)\rangle\langle\psi_n(\mu)|, \tag{A2}$$

where $|\psi_n(\mu)\rangle$ has the form of

$$|\psi_n(\mu)\rangle = \sum_{k=0}^{n} \sqrt{P_{k,A}(\mu)P_{n-k,B}(\mu)}|k\rangle_A|n-k\rangle_B. \tag{A3}$$

After normalization, the form of ρ_{AB} is eventually obtained as

$$\rho_{AB} = \sum_n p_n(\mu)|\psi'_n\rangle\langle\psi'_n|, \tag{A4}$$

in which

$$|\psi'_n\rangle = \frac{1}{\sqrt{p_n(\mu)}} \sum_{k=0}^{n} \sqrt{P_{k,A}(\mu)P_{n-k,B}(\mu)}e^{ik\Delta\phi}|k\rangle_A|n-k\rangle_B \tag{A5}$$

is the n-photon part of ρ_{AB}, and

$$p_n(\mu) = \sum_{k=0}^{n} P_{k,A}(\mu)P_{n-k,B}(\mu) \tag{A6}$$

is the probability of n-photon.

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
2. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
3. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195. [CrossRef]
4. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. [CrossRef]
5. Lo, H.-K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **2014**, *8*, 595–604. [CrossRef]
6. Pirandola, S.; Vitali, D.; Tombesi, P.; Lloyd, S. Macroscopic entanglement by entanglement swapping. *Phys. Rev. Lett.* **2006**, *97*, 150403. [CrossRef]
7. Braunstein, S.L.; Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502. [CrossRef]
8. Lo, H.-K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
9. Xu, F.; Curty, M.; Qi, B.; Lo, H.-K. Practical aspects of measurement-device-independent quantum key distribution. *New J. Phys.* **2013**, *15*, 113007. [CrossRef]
10. Zhou, Y.-H.; Yu, Z.-W.; Wang, X.-B. Tightened estimation can improve the key rate of measurement-device-independent quantum key distribution by more than 100%. *Phys. Rev. A* **2014**, *89*, 052325. [CrossRef]
11. 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]
12. Ma, X.; Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **2012**, *86*, 062319. [CrossRef]
13. Rubenok, A.; Slater, J.A.; Chan, P.; Lucio-Martinez, I.; Tittel, W. Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks. *Phys. Rev. Lett.* **2013**, *111*, 130501. [CrossRef] [PubMed]

14. Fu, Y.; Yin, H.-L.; Chen, T.-Y.; Chen, Z.-B. Long-Distance Measurement-Device-Independent Multiparty Quantum Communication. *Phys. Rev. Lett.* **2015**, *114*, 090501. [CrossRef]
15. Yin, H.-L.; Chen, T.-Y.; Yu, Z.-W.; Liu, H.; You, L.-X.; Zhou, Y.-H.; Chen, S.J.; Mao, Y.Q.; 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]
16. 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]
17. Zhang, Y.-C.; Li, Z.; Yu, S.; Gu, W.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution using squeezed states. *Phys. Rev. A* **2014**, *90*, 052325.; [CrossRef]
18. Pirandola, S.; Ottaviani, C.; Spedalieri, G.; Weedbrook, C.; Braunstein, S.L.; Lloyd, S.; Gehring, T.; Jacobsen, C.S.; Andersen, U.L. High-rate measurement-device-independent quantum cryptography. *Nat. Photonics* **2015**, *9*, 397. [CrossRef]
19. Xu, B.; Li, Z.; Yang, J.; Wei, S.; Su, Q. Huang, W.; Zhang, Y.; Guo, H. High speed continuous variable source-independent quantum random number generation. *Quantum Sci. Technol.* **2019**, *4*, 025013. [CrossRef]
20. Hwang, W.-Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef]
21. 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]
22. 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]
23. Ma, X.; Zeng, P.; Zhou, H. Phase-Matching Quantum Key Distribution. *Phys. Rev. X* **2018**, *8*, 031043. [CrossRef]
24. Tamaki, K.; Lo, H.-K.; Wang, W.Y.; Lucamarini, M. Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. *arXiv* **2018**, arXiv:1805.05511.
25. Curty, M.; Azuma, K.; Lo, H.-K. Simple security proof of twin-field type quantum key distribution protocol. *NPJ Quantum Inform.* **2019**, *5*, 64. [CrossRef]
26. Grasselli, F.; Curty, M. Practical decoy-state method for twin-field quantum key distribution. *New J. Phys.* **2019**, *21*, 073001. [CrossRef]
27. Yu, Z.-W.; Hu, X.-L.; Jiang, C.; Hu, H.; Wang, X.-B. Sending-or-not-sending twin-field quantum key distribution in practice. *Sci. Rep.* **2019**, *9*, 3080. [CrossRef]
28. Minder, M.; Pittaluga, M.; Roberts, G.L.; Lucamarini, M.; Dynes, J.F.; Yuan, Z.L.; Shields, A.J. Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nat. Photonics* **2019**, *13*, 334. [CrossRef]
29. Wang, S.; He, D.-Y.; Yin, Z.-Q.; Lu, F.-Y.; Cui, C.-H.; Chen, W.; Zhou, Z.; Guo, G.-C.; Han, Z.-F. Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System. *Phys. Rev. X* **2019**, *9*, 021046.; [CrossRef]
30. Wang, X.-B.; Hu, X.-L.; Yu, Z.-W. Effective Eavesdropping to Twin-Field Quantum Key Distribution. *arXiv* **2018**, arXiv:1805.02272.
31. Wang, X.-B. Decoy-state quantum key distribution with large random errors of light intensity. *Phys. Rev. A* **2007**, *75*, 052301. [CrossRef]
32. Gisin, N.; Fasel, S.; Kraus, B.; Zbinden, H.; Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **2006**, *73*, 022320. [CrossRef]
33. Zhao, Y.; Qi, B.; Lo, H.-K. Quantum key distribution with an unknown and untrusted source. *Phys. Rev. A* **2008**, *77*, 052327. [CrossRef]
34. Peng, X.; Jiang, H.; Xu, B.; Ma, X.; Guo, H. Experimental quantum-key distribution with an untrusted source. *Opt. Lett.* **2008**, *33*, 2077–2079. [CrossRef] [PubMed]
35. Peng, X.; Xu, B.; Guo, H. Passive-scheme analysis for solving the untrusted source problem in quantum key distribution. *Phys. Rev. A* **2010**, *81*, 042320. [CrossRef]
36. Xu, B.; Peng, X.; Guo, H. Passive scheme with a photon-number-resolving detector for monitoring the untrusted source in a plug-and-play quantum-key-distribution system. *Phys. Rev. A* **2010**, *82*, 042301.; [CrossRef]
37. Wang, G.; Li, Z.; Qiao, Y.; Chen, Z.; Peng, X.; Guo, H. Light Source Monitoring in Quantum Key Distribution With Single-Photon Detector at Room Temperature. *IEEE J. Quantum Electron.* **2018**, *54*, 9300110. [CrossRef]

38. Qiao, Y.; Wang, G.; Li, Z.; Xu, B.; Guo, H. Monitoring an untrusted light source with single-photon detectors in measurement-device-independent quantum key distribution. *Phys. Rev. A* **2019**, *99*, 052302. [CrossRef]
39. Wang, X.-B.; Peng, C.-Z.; Zhang, J.; Yang, L.; Pan, J.-W. General theory of decoy-state quantum cryptography with source errors. *Phys. Rev. A* **2008**, *77*, 042311. [CrossRef]
40. 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]
41. Xu, F.; Zhang, Y.; Zhou, Z.; Chen, W.; Han, Z.; Guo, G. Experimental demonstration of counteracting imperfect sources in a practical one-way quantum-key-distribution system. *Phys. Rev. A* **2009**, *80*, 062309. [CrossRef]