




Article

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

Xuerui Qian^{1,2,3,†}, Chunhui Zhang^{1,2,3,†} , Huawei Yuan^{1,2,3}, Xingyu Zhou^{1,2,3} , Jian Li^{1,2,3} and Qin Wang^{1,2,3,*} 

¹ Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China; quentin_qxr@163.com (X.Q.); chz@njupt.edu.cn (C.Z.); jyyhw77@163.com (H.Y.); xyz@njupt.edu.cn (X.Z.); jianli@njupt.edu.cn (J.L.)

² Broadband Wireless Communication and Sensor Network Technology, Key Lab of Ministry of Education, NUPT, Nanjing 210003, China

³ Telecommunication and Networks, National Engineering Research Center, NUPT, Nanjing 210003, China

* Correspondence: qinw@njupt.edu.cn

† These authors contributed equally to this work.

Abstract: Twin-field quantum key distribution (TF-QKD) can break the repeaterless linear bound and possess the measurement-device-independent security, and thus seems very promising in practical applications of quantum secure communication. In most reported TF-QKD protocols, light sources are assumed to possess trusted and fixed photon number distributions (PND), which are unrealistic assumptions in practical applications. Fortunately, the light source monitoring (LSM) method is proposed to circumvent this problem by actively adjusting the attenuation coefficient and monitoring the photon number distribution of light sources. However, the active light source monitoring (ALSM) method may induce additional modulation errors due to imperfect attenuation devices, deteriorating practical performances of TF-QKD systems. In this manuscript, we propose a passive light source monitoring (PLSM) scheme for TF-QKD, and employ the sending-or-not-sending (SNS) TF-QKD as an example for illustration. Simulation results show that our present work can greatly exceed both the original SNS protocol and the ALSM scheme when light source fluctuations and modulation errors are taken into account.

Keywords: twin-field quantum; sending-or-not-sending; passive light source monitoring



Citation: Qian, X.; Zhang, C.; Yuan, H.; Zhou, X.; Li, J.; Wang, Q. Passive Light Source Monitoring for Sending or Not Sending Twin-Field Quantum Key Distribution. *Entropy* **2022**, *24*, 592. <https://doi.org/10.3390/e24050592>

Academic Editor: Alberto Porzio

Received: 24 March 2022

Accepted: 21 April 2022

Published: 23 April 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Quantum key distribution (QKD) allows two legitimate parties, Alice and Bob, to share secure keys based on the laws of quantum physics. The security of BB84 protocol was proven in theory by many scientists [1–7]. However, there are still some loopholes in the measurement devices. To remove those attacks directed on the measurement devices, the measurement-device-independent quantum key distribution (MDI-QKD) [8] was put forward. Thereafter, a lot of related experiments and theories have been done on MDI-QKD, making it more efficient and practical [9–13]—just its key rate is still limited by the fundamental limit of channel capacities without quantum repeaters, e.g., the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound [14,15].

Recently, Lucamarini et al. proposed the twin-field quantum key distribution (TF-QKD) protocol [16], which can break the PLOB bound [14,15] and make the rate distance dependence change from a linear to square root. Up to date, many variants of TFQKD protocols have been proposed and experimentally demonstrated [17–28]. However, some assumptions are made for the sources in most reported works, i.e., with a trusted and fixed photon-number distribution (PND), which usually can not be satisfied in practical implementations. Those unreasonable assumptions will inevitably compromise the security of practical QKD systems. To solve the problem, the light source monitoring (LSM) method was put forward and experimentally realized by actively modulating local attenuator into

different losses [29,30], hereafter called the active light source monitoring (ALSM) scheme. However, unfortunately, the ALSM scheme will bring new loopholes and then deteriorate practical performances of TF-QKD systems during intensity modulation processes due to imperfections of attenuated devices.

In this paper, we propose a passive light source monitoring (PLSM) scheme for TF-QKD, which is accomplished by a passive monitoring module consisting of a beam splitter and two detectors at the source side. Through the PLSM module, we can obtain four monitoring events by two local detectors and then precisely estimate the bounds of source distributions. Specifically, we employ the sending-or-not-sending (SNS) TFQKD [18,31–33] as an example for illustration. Compared with the ALSM method, our PLSM method can passively monitor the PND and dramatically exceed the performance of ALSM when modulation errors are considered.

2. PLSM Scheme in SNS–TFQKD

In this section, we describe the SNS–TFQKD scheme [18,31–33] with PLSM. The schematic of the setup is shown in Figure 1, where it involves two senders, Alice and Bob, and one untrustworthy third party (UTP), Charlie. The detailed process of the SNS–TFQKD with a four-intensity decoy-state PLSM scheme can be described as follows:

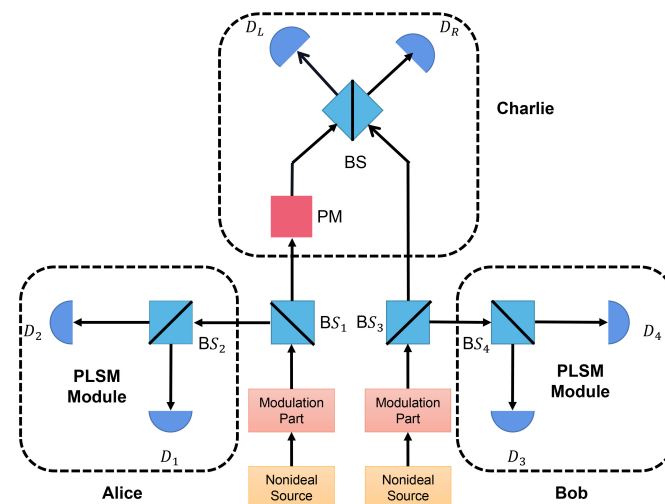


Figure 1. Schematic of the SNS–TFQKD system with PLSM. The PLSM module consists of a beam splitter (BS) and two local single-photon detectors.

Step 1. Alice and Bob do some preparatory work before sending the pulse: they send a reference coherent light to Charlie, and Charlie performs phase compensation.

Step 2. The N pulses generated by Alice and Bob are encoded by a modulation module, which contains a phase modulator (PM) and an intensity modulator (IM). During this process, each pulse is randomly chosen as the X (decoy) or Z (signal) window. At any time window i , Alice (Bob) independently determines whether it is a decoy window or a signal window. If the decoy window is chosen, she (he) prepares state $|\sqrt{v_k}e^{i\delta_{Ai}+i\gamma_{Ai}}\rangle$ ($|\sqrt{v_k}e^{i\delta_{Bi}+i\gamma_{Bi}}\rangle$) and sends it to Charlie, v_k ($k = 0, 1, 2$). If the signal window is selected, Alice (Bob) sends states $|\sqrt{u}e^{i\delta_{Ai}+i\gamma_{Ai}}\rangle$ ($|\sqrt{u}e^{i\delta_{Bi}+i\gamma_{Bi}}\rangle$) to Charlie with a probability of ε , and with a probability of $(1 - \varepsilon)$ for not sending, where the γ_A, γ_B are global phases of the coherent states.

Step 3. The pulses are split into two modes, where the idler mode is for performing PLSM and the signal mode is for encoding information and sending it to Charlie. The idler mode is further split by a local beam splitter and then sent into two local detectors. As a result, four detection events can be obtained. For example, in Alice’s PLSM module, these events can be denoted as l ($l = x, y, z, w$): x , neither D_1 or D_2 clicks; y , only D_1 clicks; z , only D_2 clicks; w , and both D_1 and D_2 click.

Step 4. Charlie measures all received states with a beam splitter and two detectors (D_L and D_R), and then announces the effective measurement outcome, i.e., which detector clicks.

Step 5. Alice and Bob announce the local detection events l and the kind of window (X window or Z window) for each pulse. In addition, the intensity and encoding phases (δ_A, δ_B) in the X basis should also be disclosed.

Step 6. Alice and Bob use the data in the X basis to estimate channel parameters, and they randomly select some bits in the Z basis for the error test and use the remaining bits to extract the final secure keys.

In this protocol, Z basis is defined as the time window when both Alice and Bob choose the signal window; X basis is denoted as the time window when both Alice and Bob choose the same decoy window (with intensity v_k), and, simultaneously, the random phases δ_A, δ_B prepared in the window satisfy

$$1 - |\cos(\delta_A - \delta_B)| \leq |\lambda|. \tag{1}$$

Here, λ is determined by the size of the phase slice chosen by Alice and Bob. In addition, the effective measurement outcome denotes that only one detector (D_L or D_R) clicks.

In the PLSM module, when the event l occurs, the idler state is projected into $\rho = \sum P_n(\mu) q_n^l |n\rangle\langle n|$, where $P_n(\mu)$ denotes the photon number distribution of the weak coherent state (WCS) with mean photon number μ ($\mu \in \{v_0, v_1, v_2, u\}$), $P_n(\mu) = e^{-\mu} \frac{\mu^n}{n!}$, and q_n^l is the probability of an n -photon state projecting into event l given by [34,35]

$$\begin{aligned} q_n^x &= (1 - d_s)^2 (1 - \eta_s)^n, \\ q_n^y &= (1 - d_s)(1 - \eta_s)^n \left[\left(1 + \frac{t\eta_s}{1 - \eta_s} \right)^n + d_s - 1 \right], \\ q_n^z &= (1 - d_s)(1 - \eta_s)^n \left[\left(\frac{1 - t\eta_s}{1 - \eta_s} \right)^n + d_s - 1 \right], \\ q_n^w &= 1 - q_n^x - q_n^y - q_n^z, \end{aligned} \tag{2}$$

where d_s and η_s are the dark counting rate and detection efficiency of the local detectors at the sender's side (Alice and Bob), respectively, and t is the transmittance of BS_2 and BS_4 . Here, for simplicity, we assume that two local detectors in PLSM module have the same detection efficiency and dark count rate, which means $\eta_1 = \eta_2 = \eta_s, d_1 = d_2 = d_s$. Define $a_n^l(\mu) := P_n(\mu) q_n^l$ as the photon number distribution under different counting events.

Then, we estimate the upper and lower bounds of probabilities of different photon-number states, i.e., the vacuum state, the one-photon state and the two-photon state. By measuring the idler mode, the gain of four events can be obtained as

$$\begin{aligned} Q_x(\mu) &= \sum a_n^x(\mu) = \sum e^{-\mu} \frac{\mu^n}{n!} (1 - d_s)^2 (1 - \eta_s)^n, \\ Q_y(\mu) &= \sum a_n^y(\mu) = \sum e^{-\mu} \frac{\mu^n}{n!} (1 - d_s)(1 - \eta_s)^n \left[\left(1 + \frac{t\eta_s}{1 - \eta_s} \right)^n + d_s - 1 \right], \\ Q_z(\mu) &= \sum a_n^z(\mu) = \sum e^{-\mu} \frac{\mu^n}{n!} (1 - d_s)(1 - \eta_s)^n \left[\left(\frac{1 - t\eta_s}{1 - \eta_s} \right)^n + d_s - 1 \right], \\ Q_w(\mu) &= \sum a_n^w(\mu) = 1 - Q_x(\mu) - Q_y(\mu) - Q_z(\mu). \end{aligned} \tag{3}$$

According to the derivation presented in Appendix A, the estimations of $P_n^L(\mu), P_n^U(\mu)$ ($n = 0, 1, 2$) are given by

$$P_0^L(\mu) = P_0^U(\mu) = \frac{Q_x(\mu)}{(1 - d_s)^2}, \tag{4}$$

$$P_1^L(\mu) = \frac{q_2^z Q_y(\mu) - q_2^y Q_z(\mu) - (q_2^z q_0^y - q_0^z q_2^y) P_0^L(\mu)}{q_2^z q_1^y - q_1^z q_2^y}, \tag{5}$$

$$P_1^U(\mu) = \frac{(q_2^y - q_3^y)Q_z(\mu) - q_2^z Q_y(\mu) + (q_2^z q_0^y - q_2^z q_3^y - q_0^z q_2^y + q_0^z q_3^y)P_0^L(\mu) + q_2^z q_3^y}{q_1^y(q_2^y - q_3^y) - q_2^y(q_1^y - q_3^y)}, \quad (6)$$

$$P_2^L(\mu) = \frac{Q_y(\mu) - (q_0^y - q_3^y)P_0^U(\mu) - (q_1^y - q_3^y)P_1^U(\mu) - q_3^y}{q_2^y - q_3^y}, \quad (7)$$

$$P_2^U(\mu) = \frac{Q_z(\mu) - q_0^z P_0^L(\mu) - q_1^z P_1^L(\mu)}{q_2^z}, \quad (8)$$

where $P_n^{L(U)}(\mu)$ represents the lower or upper bounds on the probability of having the n -photon state given the mean photon number μ .

In the SNS–TFQKD, Alice and Bob simultaneously send photon pulses to the untrustworthy third party (UTP) Charlie. According to Ref. [36], the decoy-state method is still applicable under unknown PND conditions; the lower bound of the single-photon counting rate and the upper bound of the single-photon error rate can be estimated as

$$s_1^L = \frac{p_2^L(v_2)[S_{v_1} - p_0^U(v_1)S_0] - p_2^U(v_1)[S_{v_2} - p_0^L(v_2)S_0]}{p_2^U(v_2)p_1^U(v_1) - p_2^L(v_1)p_1^L(v_2)}, \quad (9)$$

$$e_1^{ph,U} = \frac{S_{v_1}E_{v_1} - p_0^L(v_1)S_0/2}{p_1^L(v_1)s_1^L}. \quad (10)$$

Here, we set $v_0 = 0, v_2 > v_1 > 0$, and S_{v_k}, E_{v_k} are the counting rate and the bit error rate of a state with intensity v_k sent in decoy windows, respectively. In addition, the relationships between $P_n^{L(U)}(\mu)$ and $p_n^{L(U)}(\mu)$ are set by [30]

$$\begin{aligned} p_0^{L(U)}(\mu) &:= [P_0^{L(U)}(\mu)]^2, p_1^{L(U)}(\mu) := 2P_0^{L(U)}(\mu)P_1^{L(U)}(\mu), \\ p_2^{L(U)}(\mu) &:= 2P_0^{L(U)}(\mu)P_2^{L(U)}(\mu) + [P_1^{L(U)}(\mu)]^2. \end{aligned} \quad (11)$$

Finally, the secure key rate is

$$R = 2\varepsilon(1 - \varepsilon)P_1^L(u)s_1^L(1 - H(e_1^{ph,U})) - S_Z fH(E_Z), \quad (12)$$

where ε represents 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; $P_1^L(u)$ is the lower bound of the probability of single photons in the signal state; S_Z and E_Z refer to the gain and the average quantum bit error of pulses with intensity u sent in signal windows.

3. Numerical Simulations and Analysis

In the following, we perform numerical simulations for the original SNS–TFQKD [18], the SNS–TFQKD with ALSM [30] and the SNS–TFQKD with PLSM. In simulations, the gain and the quantum bit error of decoy states in X basis in Equations (9) and (10) are expressed as

$$\begin{aligned} S_{v_k} &= S_{v_k}^C + S_{v_k}^E, \\ S_{v_k}E_{v_k} &= E_{opt}S_{v_k}^C + (1 - E_{opt})S_{v_k}^E, \\ S_{v_k}^C &= \frac{1}{\Delta}(1 - P_{dc}) \int_{-\Delta/2}^{\Delta/2} e^{-v_k\eta(1 - \cos\delta)} d\delta - (1 - P_{dc})^2 e^{-2v_k\eta}, \\ S_{v_k}^E &= \frac{1}{\Delta}(1 - P_{dc}) \int_{-\Delta/2}^{\Delta/2} e^{-v_k\eta(1 + \cos\delta)} d\delta - (1 - P_{dc})^2 e^{-2v_k\eta}, \end{aligned} \quad (13)$$

where $S_{v_k}^C(S_{v_k}^E)$ is the counting rate of twin-field states entering into the correct (wrong) detector; $\eta = \eta_D 10^{-\frac{\alpha s}{20}}$ denotes the total channel transmittance, where α and s are the loss coefficient and the length of channels, respectively; η_D and P_{dc} each refer to the efficiency and the dark count rate of detectors at Charlie’s side, respectively. $\delta = |\delta_B - \delta_A|$ is the phase difference between the twin-field states prepared by Alice and Bob; $\Delta = 2\pi/M$ is the size of the phase slice and M is the number of phase slices; E_{opt} represents the optical misalignment error, S_0 is the counting rate of the vacuum state, and $S_0 = 2P_{dc}(1 - P_{dc})$. The average quantum bit error and the counting rate for the signal states can be respectively expressed as:

$$\begin{aligned} S_Z E_Z &= 2P_{dc}(1 - P_{dc})(1 - \epsilon)^2 + 2\epsilon^2(1 - P_{dc})e^{-u\eta} [I_0(u\eta) - (1 - P_{dc})e^{-u\eta}], \\ S_Z &= 4\epsilon(1 - \epsilon)(1 - P_{dc})e^{-\frac{u\eta}{2}} \left[1 - (1 - P_{dc})e^{-\frac{u\eta}{2}} \right] + S_Z E_Z. \end{aligned} \tag{14}$$

Here, $I_0(x)$ is the 0-order hyperbolic Bessel function of the first kind [31].

In the following, we do comparisons among three schemes, the original SNS–TFQKD, the ALSM SNS–TFQKD, and the present PLSM SNS–TFQKD, by using either ideal light sources without intensity fluctuations or practical light sources with intensity fluctuations. In addition, we also analyze the effect of modulation error on the ALSM scheme. The basic device parameters are shown in Table 1 [30].

Table 1. The basic system parameters used in our numerical simulations. α : the loss coefficient of fiber at telecommunication wavelength (dB/km); η_D and P_{dc} are the efficiency and dark count rate of detectors at Charlie’s side; E_{opt} : the misalignment error of the QKD system; f : the error correction efficiency; M : the number of phase slices.

	α	M	η_D	P_{dc}	E_{opt}	f
set <i>a</i>	0.2 dB/km	16	80%	10^{-11}	1%	1.1
set <i>b</i>	0.2 dB/km	16	30%	10^{-9}	3%	1.15

In ALSM, the attenuation coefficients are set as $\eta_0 = 1, \eta_1 = 0.95, \eta_2 = 0.9$. For a fair comparison, in our scheme, the detection efficiency in PLSM module is set as $\eta_s = 0.9$. In addition, the dark count rate of local detectors d_s in ALSM and PLSM is set with the same value denoted as P_{dc} as listed in row *a* of Table 1. In addition, we adopt the local search algorithm (LSA) [9] to optimize the parameters $\epsilon, t, v_0, v_1, v_2, u$. The numerical simulation results are presented in Figures 2–4.

The performance of different monitoring methods with ideal sources without intensity fluctuations are presented in Figure 2. Simulation results show that the performance of our proposed PLSM SNS–TFQKD is comparable to both the original SNS–TFQKD and the ALSM SNS–TFQKD. It is also clear that the maximum transmission distance of all schemes exceeds 800 km. In addition, if actively odd-parity pairing (AOPP) [33] of post data processing is adopted, it can further improve the distance and key rate of SNS–TFQKD significantly.

However, in realistic implementations, the fluctuation of light sources is a common phenomenon in QKD systems [37,38]; therefore, it should be taken into account. In general, the signal from light sources can be considered as a coherent state, whose intensity usually possesses a Gaussian distribution:

$$G(\mu) = \frac{1}{\sqrt{2\pi}\sigma_\mu} \exp\left[-\frac{(\mu - \mu_0)^2}{2\sigma_\mu^2}\right], \tag{15}$$

where μ_0 and σ_μ represent the mean value and standard deviation, respectively. Define the fluctuation coefficient as $\sigma := \sigma_\mu / \mu_0$, and $Q_I(\mu)$ can be rewritten as

$$Q_I(\mu_0) = \int Q_I(\mu)G(\mu)d\mu. \tag{16}$$

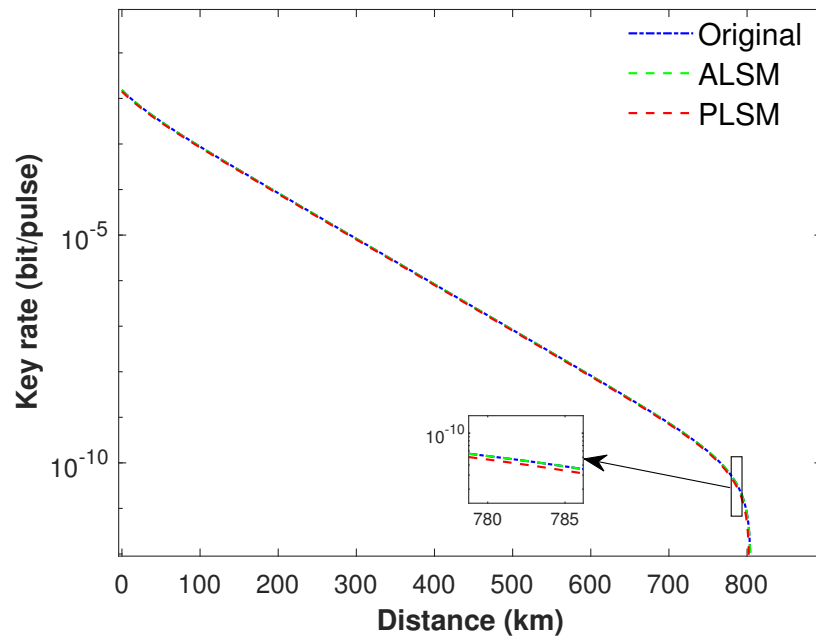


Figure 2. The secure key rate of different monitoring method using a set of parameters in row *a* of Table 1. The blue solid curve represents the original SNS–TFQKD; the red dash curve denotes our present PLSM SNS–TFQKD; and the green dash curve is the ALSM SNS–TFQKD. In addition, the variation trend of the key rate ranging between 780 km and 785 km is illustrated in the inset. It shows that our proposal can offer a key rate comparable to both the original SNS–TFQKD and the ALSM SNS–TFQKD when using photon sources without fluctuations.

After calculating and simplifying, the counting rate of four events can be reformulated as

$$\begin{aligned} Q_x(\mu_0) &= (1 - d_s)^2 \exp\left[\frac{1}{2}\eta_s(-2\mu_0 + \eta_s\sigma_\mu^2)\right], \\ Q_y(\mu_0) &= (1 - d_s) \exp\left(-\frac{\mu_0^2}{2\sigma_\mu^2}\right) \left\{ (1 - d_s) \exp\left[\frac{(\mu_0 - \eta_s\sigma_\mu^2)^2}{2\sigma_\mu^2}\right] - \exp\left[\frac{(\mu_0 - (1 - t)\eta_s\sigma_\mu^2)^2}{2\sigma_\mu^2}\right] \right\}, \\ Q_z(\mu_0) &= (1 - d_s) \exp\left(-\frac{\mu_0^2}{2\sigma_\mu^2}\right) \left\{ (1 - d_s) \exp\left[\frac{(\mu_0 - \eta_s\sigma_\mu^2)^2}{2\sigma_\mu^2}\right] - \exp\left[\frac{(\mu_0 - t\eta_s\sigma_\mu^2)^2}{2\sigma_\mu^2}\right] \right\}, \\ Q_w(\mu_0) &= 1 - Q_x(\mu_0) - Q_y(\mu_0) - Q_z(\mu_0). \end{aligned} \tag{17}$$

On the other hand, $S_{v_k}^C$ and $S_{v_k}^E$ will change if light fluctuations are considered, which can be expressed as [36]

$$\begin{aligned} \widehat{S}_{v_k}^C &= \int S_{v_k}^C G(v_k)dv_k = \int \left[\frac{1}{\Delta}(1 - P_{dc}) \int_{-\Delta/2}^{\Delta/2} e^{-v_k\eta(1-\cos\delta)}d\delta - (1 - P_{dc})^2 e^{-2v_k\eta} \right] G(v_k)dv_k, \\ \widehat{S}_{v_k}^E &= \int S_{v_k}^E G(v_k)dv_k = \int \left[\frac{1}{\Delta}(1 - P_{dc}) \int_{-\Delta/2}^{\Delta/2} e^{-v_k\eta(1+\cos\delta)}d\delta - (1 - P_{dc})^2 e^{-2v_k\eta} \right] G(v_k)dv_k. \end{aligned} \tag{18}$$

Then, the counting rate and the quantum bit error of decoy states in X basis can be respectively re-expressed as

$$\begin{aligned} \hat{S}_{v_k} &= \hat{S}_{v_k}^C + \hat{S}_{v_k}^E, \\ \hat{S}_{v_k} \hat{E}_{v_k} &= E_{opt} \hat{S}_{v_k}^C + (1 - E_{opt}) \hat{S}_{v_k}^E. \end{aligned} \tag{19}$$

Then, s_1^L and $e_1^{ph,U}$ can be rewritten as [7]

$$s_1^L = \frac{p_2^L(v_2) [\hat{S}_{v_1} - p_0^U(v_1) S_0] - p_2^U(v_1) [\hat{S}_{v_2} - p_0^L(v_2) S_0]}{p_2^U(v_2) p_1^U(v_1) - p_2^L(v_1) p_1^L(v_2)}, \tag{20}$$

$$e_1^{ph,U} = \frac{\hat{S}_{v_1} \hat{E}_{v_1} - p_0^L(v_1) S_0 / 2}{p_1^L(v_1) s_1^L}. \tag{21}$$

In the following, we compare the performance of SNS–TFQKD with various schemes under different fluctuation coefficients σ .

In order to simulate the realistic condition, we use a set of practical system parameters in row b of Table 1 [16]. In the realistic condition, the coefficient of light intensity fluctuation σ is usually greater than 1% [39]; therefore, we set coefficient of intensity fluctuations as $\sigma = 1\%$ and $\sigma = 2\%$.

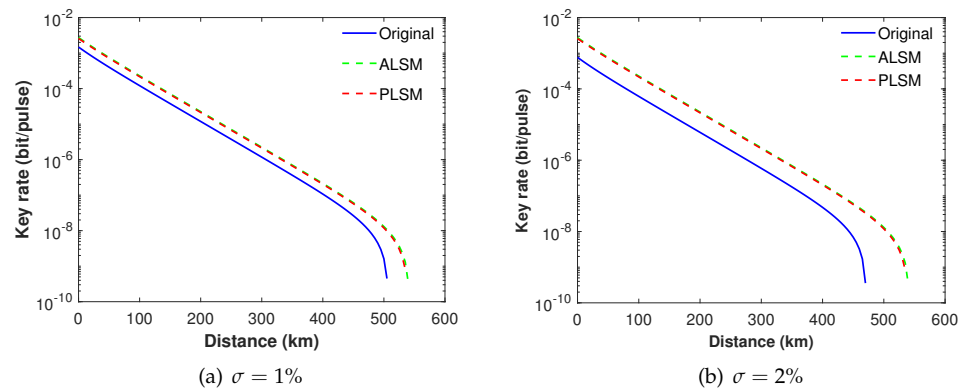


Figure 3. The secure key rate of different schemes with intensity fluctuation $\sigma = 1\%$ in (a) and $\sigma = 2\%$ in (b) when intensity modulation errors are not taken into account.

As we can see from Figure 3a,b, when intensity fluctuations are taken into account, both ALSM and our present PLSM can show much better performance compared with the original SNS TF-QKD protocol. For example, when $\sigma = 1\%$ or 2% , both ALSM and our present PLSM only slightly decrease its key rate and transmission distance, while the original SNS TF-QKD protocol rapidly drops its key rate and transmission distance.

In practice, when switching between different coefficients, it may bring into modulation errors in the ALSM scheme. We define the attenuation coefficients modulation error as Ω , then $\eta^U = \eta(1 + \Omega)$, $\eta^L = \eta(1 - \Omega)$, where η^U and η^L are the upper bound and lower bound of attenuation coefficients. Based on [30], $P_n^{L(U)}(\mu)$ in ALSM has been reestimated in Appendix B. The simulation results are shown in Figure 4, and it is obvious that our scheme can show much better performance than the ALSM scheme when the modulation error is accounted. For example, when we reasonably set $\Omega = 0.02\%$, the maximum transmission distance drops from 540 km to 435 km for the ALSM scheme, while it still remains constant for our PLSM scheme. Obviously, the ALSM scheme is very susceptible to intensity modulation errors.

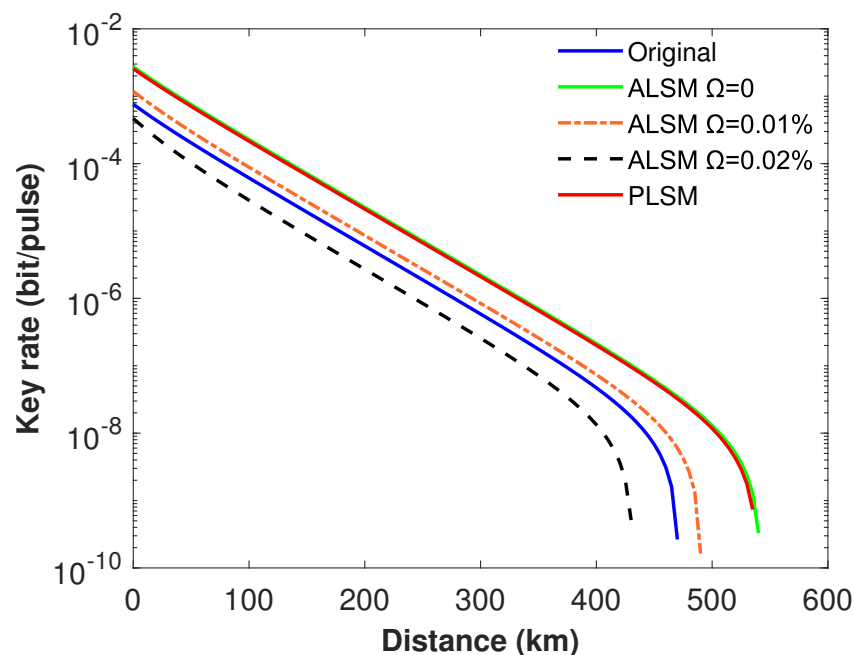


Figure 4. The secure key rate of different monitoring methods when different modulation errors are taken into account. Here, parameters in line *b* of Table 1 and the intensity fluctuation $\delta = 2\%$ are used. The blue solid curve represents the original SNS–TFQKD; the green solid curve is the ALSM SNS–TFQKD when $\Omega = 0$; the red solid curve denotes the PLSM SNS–TFQKD; the orange dotted-dash curve and the black dash curve denote the ALSM SNS–TFQKD with modulation errors $\Omega = 0.01\%$ and $\Omega = 0.02\%$, respectively.

4. Conclusions

In this paper, we propose a PLSM scheme for TF-QKD, which is accomplished by implementing a passive monitoring module consisting of a beam splitter and two detectors at the source side. Through the PLSM module, we can obtain four kinds of monitoring events with two local detectors and can then precisely estimate the bounds of source distributions. We build a theoretical model and carry out corresponding numerical simulations. Simulation results show that our present work can outperform the original SNS–TFQKD protocol when there are existing intensity fluctuations in the light sources. Moreover, it shows much better performance than the reported ALSM scheme when modulation errors are taken into account. Therefore, our present work can not only reduce assumptions on the source distribution in former TF-QKD protocols, but also close the additional loopholes existing in the former active monitoring scheme, and thus seems very promising in practical implementations of QKD in the near future.

Author Contributions: Conceptualization, C.Z., H.Y., X.Z., J.L. and Q.W.; Writing—original draft, X.Q.; Writing—review & editing, X.Q. All authors have read and agreed to the published version of the manuscript.

Funding: We gratefully acknowledge the financial support from the National Key R&D Program of China (2018YFA0306400, 2017YFA0304100), the National Natural Science Foundation of China (12074194, U19A2075, 12104240, 62101285), the Leading-edge technology Program of Jiangsu Natural Science Foundation (BK20192001), the Natural Science Foundation of Jiangsu Province (BK20210582), NUPTSF (NY220122, NY220123), and the Postgraduate Research & Practice Innovation Program of Jiangsu Province (SJCX21_0260).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors are grateful to the anonymous reviewers for their constructive suggestions and comments

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

Appendix A. Upper Bound and Lower Bound of $P_n(\mu)$ in PLSM

In this appendix, in order to obtain $P_n^{L(U)}(\mu)$, we use the gain of four events by measuring the idler mode:

$$Q_x(\mu) = \sum P_n(\mu)q_n^x, \tag{A1}$$

$$Q_y(\mu) = \sum P_n(\mu)q_n^y, \tag{A2}$$

$$Q_z(\mu) = \sum P_n(\mu)q_n^z, \tag{A3}$$

$$Q_w(\mu) = 1 - Q_x(\mu) - Q_y(\mu) - Q_z(\mu). \tag{A4}$$

With Equation (A1), we have

$$Q_x(\mu) = \sum P_n(\mu)(1 - d_s)^2(1 - \eta_s)^n. \tag{A5}$$

When setting $\eta_s = 1$, we can obtain

$$P_0^L(\mu) = P_0^U(\mu) = \frac{Q_x(\mu)}{(1 - d_s)^2}. \tag{A6}$$

Combining Equations (A2) and (A3) to eliminate the parameter $P_2(\mu)$:

$$\begin{aligned} q_2^z Q_y(\mu) - q_2^y Q_z(\mu) &= P_0(\mu)(q_0^y q_2^z - q_2^y q_0^z) + P_1(\mu)(q_1^y q_2^z - q_2^y q_1^z) + \sum_{i=3}^{\infty} P_i(\mu)(q_2^z q_i^y - q_i^z q_2^y) \\ &\leq P_0(\mu)(q_0^y q_2^z - q_2^y q_0^z) + P_1(\mu)(q_1^y q_2^z - q_2^y q_1^z), \end{aligned} \tag{A7}$$

then $P_1^L(\mu)$ is obtained as

$$P_1^L(\mu) = \frac{q_2^z Q_y(\mu) - q_2^y Q_z(\mu) - (q_2^z q_0^y - q_0^z q_2^y) P_0^L(\mu)}{q_2^z q_1^y - q_1^z q_2^y}. \tag{A8}$$

According to Equations (A1) and (A2), we scale appropriately and change the equation to an inequality as

$$\sum P_n(\mu)q_n^y \geq P_0(\mu)q_0^y + P_1(\mu)q_1^y + P_2(\mu)q_2^y, \tag{A9}$$

$$\sum P_n(\mu)q_n^z \geq P_0(\mu)q_0^z + P_1(\mu)q_1^z + P_2(\mu)q_2^z, \tag{A10}$$

$$\sum P_n(\mu)q_n^y \leq P_0(\mu)q_0^y + P_1(\mu)q_1^y + P_2(\mu)q_2^y + q_3^y(1 - P_0(\mu) - P_1(\mu) - P_2(\mu)), \tag{A11}$$

$$\sum P_n(\mu)q_n^z \leq P_0(\mu)q_0^z + P_1(\mu)q_1^z + P_2(\mu)q_2^z + q_3^z(1 - P_0(\mu) - P_1(\mu) - P_2(\mu)). \tag{A12}$$

Using Equations (A9) and (A12) to eliminate the parameter $P_2(\mu)$, we obtain the upper bound of $P_1(\mu)$

$$P_1^U(\mu) = \frac{(q_2^y - q_3^y)Q_z(\mu) - q_2^z Q_y(\mu) + (q_2^z q_0^y - q_2^z q_3^y - q_0^z q_2^y + q_0^z q_3^y)P_0^L(\mu) + q_2^z q_3^y}{q_1^y(q_2^y - q_3^y) - q_2^y(q_1^y - q_3^y)}. \tag{A13}$$

The lower bound of $P_2(\mu)$ can be obtained by using $P_0^U(\mu)$ and $P_1^U(\mu)$ in Equation (A11), and the upper bound $P_2(\mu)$ can be obtained by using $P_0^L(\mu)$ and $P_1^L(\mu)$ in Equation (A9):

$$P_2^L(\mu) = \frac{Q_y(\mu) - (q_0^y - q_3^y)P_0^U(\mu) - (q_1^y - q_3^y)P_1^U(\mu) - q_3^y}{q_2^y - q_3^y}, \tag{A14}$$

$$P_2^U(\mu) = \frac{Q_z(\mu) - q_0^z P_0^L(\mu) - q_1^z P_1^L(\mu)}{q_2^z}. \tag{A15}$$

Appendix B. Upper Bound and Lower Bound Of $P_n(\mu)$ in ALSM

According to Ref. [29], we set $Q^\mu(\eta_k)$ as the probabilities of the single photon detector not responding with η_k for source μ , which can be described as

$$Q^\mu(\eta_0) = (1 - Y_0) \sum_{n=0} (1 - \eta_0)^n P_n(\mu), \tag{A16}$$

$$Q^\mu(\eta_1) = (1 - Y_0) \sum_{n=0} (1 - \eta_1)^n P_n(\mu), \tag{A17}$$

$$Q^\mu(\eta_2) = (1 - Y_0) \sum_{n=0} (1 - \eta_2)^n P_n(\mu), \tag{A18}$$

and then we set $\eta_k^U = \max\{\eta_k(1 + \Omega), 1\}$, $\eta_k^L = \eta_k(1 - \Omega)$ ($k = 0, 1, 2$). When considering the modulation errors, $P_n^{L(U)}(\mu)$ ($n = 0, 1, 2$) can be reestimated as

$$P_0^L(\mu) = \frac{Q^\mu(\eta_0^U)}{1 - Y_0}, P_0^U(\mu) = \frac{Q^\mu(\eta_0^L)}{1 - Y_0}, \tag{A19}$$

$$P_1^L(\mu) = \frac{(1 - \eta_2^L)^2 Q^\mu(\eta_1^L) - (1 - \eta_1^L)^2 Q^\mu(\eta_2^L)}{(1 - Y_0)(1 - \eta_1^L)(1 - \eta_2^L)(\eta_1^L - \eta_2^L)} - \left(\frac{1}{1 - \eta_1^L} + \frac{1}{1 - \eta_2^L} \right) P_0^U(\mu), \tag{A20}$$

$$P_1^U(\mu) = \frac{(1 - \eta_2^U)(1 - \eta_1^L)}{[1 - \eta_2^U - (1 - \eta_1^L)(2 - \eta_2^U)]} \left\{ \frac{Q^\mu(\eta_1^L)}{(1 - \eta_1^L)^2(1 - Y_0)} + \frac{[1 - (1 - \eta_2^U)^3]}{\eta_2^U(1 - \eta_2^U)^2} P_0^U(\mu) \right. \\ \left. + \frac{1 - \eta_2^U}{\eta_2^U} - \frac{Q^\mu(\eta_2^U)}{\eta_2^U(1 - \eta_2^U)^2(1 - Y_0)} - \frac{P_0^U(\mu)}{(1 - \eta_1^L)^2} \right\}, \tag{A21}$$

$$P_2^L(\mu) = \frac{Q^\mu(\eta_2^L)}{(1 - Y_0)(1 - \eta_2^L)^2 \eta_2^L} - \frac{1 - \eta_2^L}{\eta_2^L} - \frac{[1 - (1 - \eta_2^L)^3]}{(1 - \eta_2^L)^2 \eta_2^L} P_0^U(\mu) - \frac{2 - \eta_2^L}{1 - \eta_2^L} P_1^U(\mu), \tag{A22}$$

$$P_2^U(\mu) = \frac{Q^\mu(\eta_2^L)}{(1 - Y_0)(1 - \eta_2^L)^2} - \frac{P_0^L(\mu)}{(1 - \eta_2^L)^2} - \frac{P_1^L(\mu)}{1 - \eta_2^L}. \tag{A23}$$

Then these reestimated PNDs are used in ALSM SNS–TFQKD to calculate the final secure rate.

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. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441. [[CrossRef](#)] [[PubMed](#)]
4. Mayers, D. Unconditional security in quantum cryptography. *JACM* **2001**, *48*, 351–406. [[CrossRef](#)]
5. Lo, H.-K.; Chau, H.-F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, *283*, 2050. [[CrossRef](#)] [[PubMed](#)]
6. Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **1992**, *5*, 3. [[CrossRef](#)]

7. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [[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.; Xu, H.; Lo, H.-K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 052333. [[CrossRef](#)]
10. 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](#)]
11. Yu, Z.-W.; Zhou, Y.-H.; Wang, X.-B. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method. *Phys. Rev. A* **2015**, *91*, 032318. [[CrossRef](#)]
12. 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](#)]
13. Jiang, C.; Yu, Z.-W.; Hu, X.-L.; Wang, X.-B. Higher key rate of measurement-device-independent quantum key distribution through joint data processing. *Phys. Rev. A* **2021**, *103*, 012402. [[CrossRef](#)]
14. 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.
15. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. [[CrossRef](#)] [[PubMed](#)]
16. 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. [[CrossRef](#)] [[PubMed](#)]
17. Ma, X.; Zeng, P.; Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X* **2018**, *8*, 031043. [[CrossRef](#)]
18. Wang, X.-B.; Yu, Z.-W.; Hu, X.-L.T. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **2018**, *98*, 062323. [[CrossRef](#)]
19. 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](#)]
20. 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](#)]
21. Lin, J.; Lütkenhaus, N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* **2018**, *98*, 042332. [[CrossRef](#)]
22. Maeda, K.; Sasaki, T.; Koashi, M. Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit. *Nat. Commun.* **2019**, *10*, 3140. [[CrossRef](#)]
23. 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](#)]
24. Liu, Y.; Yu, Z.-W.; Zhang, W.; Guan, J.Y.; Chen, J.-P.; Zhang, C.; Hu, X.-L.; Li, H.; Chen, T.-Y.; You, L.; et al. Experimental twin-field quantum key distribution through sending or not sending. *Phys. Rev. Lett.* **2019**, *123*, 100505. [[CrossRef](#)] [[PubMed](#)]
25. 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](#)]
26. Zhong, X.; Hu, J.; Curty, M.; Qian, L.; Lo, H.-K. Proof-of-principle experimental demonstration of twin-field type quantum key distribution. *Phys. Rev. Lett.* **2019**, *123*, 100506. [[CrossRef](#)] [[PubMed](#)]
27. Fang, X.-T.; Zeng, P.; Liu, H. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nat. Photonics* **2020**, *14*, 422. [[CrossRef](#)]
28. Chen, J.-P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.; Hu, X.L.; Guan, J.-Y.; Yu, Z.-W.; Xu, H.; Lin, J.; et al. Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km. *Phys. Rev. Lett.* **2020**, *124*, 070501. [[CrossRef](#)]
29. 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](#)]
30. Qiao, Y.; Wang, G.; Li, Z.; Xu, B.; Guo, H. Sending-or-not-sending twin-field quantum key distribution with light source monitoring. *Entropy* **2019**, *22*, 36. [[CrossRef](#)] [[PubMed](#)]
31. 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](#)]
32. Zhang, C.H.; Zhang, C.M.; Wang, Q. Twin-field quantum key distribution with modified coherent states. *Opt. Lett.* **2019**, *44*, 1468–1471. [[CrossRef](#)]
33. 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](#)]
34. 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](#)]
35. 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. [[CrossRef](#)] [[PubMed](#)]

36. 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](#)]
37. 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](#)]
38. Wang, X.-B. Decoy-state quantum key distribution with large random errors of light intensity. *Phys. Rev. A* **2007**, *75*, 052301. [[CrossRef](#)]
39. 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](#)]