entropy

IMPACT FACTOR 2.0

Indexed in: PubMed

CITESCORE 5.2

Article

An Effective Parameter Analysis for Sending-or-Not-Sending Quantum Key Distribution with Untrusted Light Sources

Jiajian Huang, Weigang Li and Yucheng Qiao

MDPI

https://doi.org/10.3390/e27060547

entropy

MDPI

Article

An Effective Parameter Analysis for Sending-or-Not-Sending Quantum Key Distribution with Untrusted Light Sources

Jiajian Huang [1], Weigang Li [2] and Yucheng Qiao [1,*]

[1] Guangxi Key Laboratory of Cryptography and Infomation Security, Guilin University of Electronic Technology, Guilin 541004, China; jiajianhuang@mails.guet.edu.cn
[2] School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, China; lwg1997@mails.guet.edu.cn
* Correspondence: glqyc251@guet.edu.cn

Abstract: The twin-field (TF) protocol is a key protocol in quantum key distribution (QKD) that enables remote key distribution, achieving a maximum secure transmission distance of over 500 km. However, the TF protocol still faces several security issues in real-world environments. To address the issue of untrusted sources, one effective solution is to introduce a light-source monitoring module into the system. Analysis shows that a solution based on untagged bits (UBs) can achieve ideal monitoring performance. This solution can capture UB signals to accurately estimate key parameters in the protocol's security analysis, ultimately deriving a tight bound for the secure bit rate. Simulations show that this solution approximates the performance of ideal light sources in the presence of untrusted sources and effectively mitigates the impact of light-source fluctuations. It outperforms other solutions in key performance metrics, such as transmission distance.

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

Academic Editor: Osamu Hirota

Received: 17 April 2025
Revised: 18 May 2025
Accepted: 18 May 2025
Published: 22 May 2025

Citation: Huang, J.; Li, W.; Qiao, Y. An Effective Parameter Analysis for Sending-or-Not-Sending Quantum Key Distribution with Untrusted Light Sources. *Entropy* **2025**, *27*, 547. https://doi.org/10.3390/e27060547

1. Introduction

Quantum key distribution (QKD) is a secure communication protocol with strong security guarantees. In 1984, the BB84 protocol [1] emerged, marking the beginning of quantum communication. Since then, various protocols have emerged, including the BBM92 protocol [2], SARG04 protocol [3], differential phase protocol [4], and six-state protocol [5]. On the other hand, rapid theoretical advancements in QKD have been accompanied by significant experimental achievements. In 1992, Bennett and Brassard successfully built the first QKD experimental system [6] and demonstrated the key distribution process of the BB84 protocol. In 1999, Bechmann-Pasquinucci and Tittel proposed the use of high-dimensional quantum qubits [7] for QKD to enhance its information-carrying capacity, replacing traditional two-dimensional qubits. In 2002, Cerf and Bourennane analyzed the security of d-level QKD systems [8]. The feasibility of high-dimensional QKD has been gradually demonstrated by researchers with studies focusing on transmission distance [9,10] and security [11–13]. Although the communication distance and key length of this system are limited, it proved that QKD is feasible. This indicates that QKD research is continuously evolving and becoming more sophisticated. However, as research progresses, scholars have identified several security vulnerabilities in QKD applications. These include the photon number-splitting (PNS) attack [14], the fake state (FS) attack [15], the time-shift (TS) attack [16], and the detector-blinding (DB) attack [17].

Scholars have proposed various methods and protocols to counter the above attacks. In 2004, Gottesman, Lo, N. Lütkenhaus, and Preskill proposed an analytical method for assessing the security of the BB84 protocol with non-ideal devices, which was known as the GLLP [18] theory. This theory effectively extends the security of the BB84 protocol to practical applications, analyzing the real-world security of QKD. Subsequent theoretical advancements, such as the decoy state method [19] and optimized parameter estimation techniques, have been developed to improve the performance of practical systems [20–22], enhancing both security and efficiency. To address side-channel attack threats faced by detectors, scholars have proposed the measurement-device-independent (MDI) protocol [23].

To improve the performance of practical QKD systems, Lucamarini et al. proposed the twin-field (TF) protocol [24] in 2018. Due to its significant advantages in transmission, it has sparked widespread research. Many subsequent enhanced protocols, referred to as TF-type protocols, further improved both the security and performance of the system. Among the TF-type protocols, sending-or-not-sending (SNS) protocol [25] is more widely used. The SNS protocol achieves long-distance secure transmission by configuring a series of sending or not sending signals. Recently, researchers have analyzed the security of the SNS protocol under different situations [26–30]. Researchers also have proposed various methods to enhance the performance of the SNS protocol. For example, by using the independent lasers [31], introducing the actively odd parity pairing (AOPP) method [32–34] and applying the phase postselection [35], the transmission range of the SNS protocol can be significantly extended. Nonetheless, practical implementation challenges persist. Researchers have addressed the practical security issues of the SNS protocol, particularly those related to the light source [36–44]. In our preliminary work, we investigated light source monitoring. Although this work is theoretically significant, it is not practical for real-world system implementation. In this paper, we propose a practical solution, untagged bits (UBs) [45], to effectively address the light source security challenges in SNS protocol.

This paper is organized as follows. In Section 2, we describe the steps of the SNS protocol, analyze its security, and estimate key parameters. In Section 3, we present numerical simulations and analyze the results. Finally, Section 4 concludes the paper.

2. SNS Protocol with UB

2.1. Introduction of SNS Protocol

Although the structure of the SNS protocol is similar to that of the TF protocol, it optimizes the signal preparation and post-processing steps. The steps of the SNS protocol are as follows [25]:

1. At each time window i, Alice (Bob) determines whether it is a signal or decoy window. If it is a decoy window, Alice (Bob) prepares a coherent state $\left|\sqrt{\mu_d}e^{i\delta+i\gamma}\right\rangle$ and sends it to Charlie. If it is a signal window, Alice (Bob) prepares a coherent state $\left|\sqrt{\mu_s}e^{i\delta+i\gamma}\right\rangle$ with probability ϵ and sends it to Charlie. μ_d and μ_s represent the photon intensity of the decoy state and the signal state, $\delta \in \{\delta_A, \delta_B\}$ represents the random phase, and $\gamma \in \{\gamma_A, \gamma_B\}$ represents the phase offset of the channel.
2. Charlie receives the states sent by Alice and Bob and publishes all the measurement results for the effective events. Effective events are defined as follows: (1) When Alice and Bob simultaneously decide on the signal window, Alice (Bob) decides to send the signal, while Bob (Alice) decides not to send it, corresponding to Charlie announcing only detector $D_{0(1)}$ clicks. (2) When Alice and Bob simultaneously decide on the decoy

window, they prepare coherent states with the same intensity, and in this window, the random phases δ_A and δ_B satisfy [25]

$$1 - |\cos(\delta_A - \delta_B)| \leqslant |\lambda|, \tag{1}$$

corresponding to Charlie announcing only detector $D_{1(0)}$ clicks. The value of λ is determined by the size of the phase slice chosen by Alice and Bob, as described in Ref. [24].

3. After Charlie publishes all the measurement results, Alice and Bob announce all the windows and the details of the decoy windows to classify the data accordingly and determine the parameters of the security key formula.
4. The secret key rate of the SNS protocol has been given as [25,26]

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

ϵ represents the probability that Alice (Bob) sends the signal state to Charlie during the signal window. $P_1^L(\mu_s)$ refers to the lower bound of the probability of sending a signal that contains a single photon. We define Z-data [26] as events in which Alice and Bob simultaneously select the signal window. Z_1-data refers to effective events where one party chooses to send the signal while the other does not. s_1^L and e_1^U represent the lower bound of the count rate and the upper bound of the phase error rate of single-photon events in the Z_1-data. S_Z and E_Z represent the count rate and bit error rate of the signal, f is the error correction efficiency, and $H(x) = -xlog_2x - (1-x)log_2(1-x)$ refers to the binary Shannon entropy function.

Under asymptotic conditions, Equation (2) remains valid and can accurately estimate the parameters s_1^L and e_1^U [25].

$$s_1 \geq s_1^L = \frac{p_2^L(\mu_2)\left[S_{\mu_1} - p_0^U(\mu_1)S_{\mu_0}\right] - p_2^U(\mu_1)\left[S_{\mu_2} - p_0^L(\mu_2)S_{\mu_0}\right]}{p_2^U(\mu_2)p_1^U(\mu_1) - p_2^L(\mu_1)p_1^L(\mu_2)}, \tag{3}$$

$$e_1 \leq e_1^U = \frac{S_{\mu_1}E_{\mu_1} - p_0^L(\mu_1)S_{\mu_0}E_{\mu_0}}{p_1^L(\mu_1)s_1^L}. \tag{4}$$

$\mu_0 = 0 < \mu_1 < \mu_2$ represents the three intensities of the decoy windows. $p_0^{L(U)}(\mu_i)$, $p_1^{L(U)}(\mu_i)$, and $p_2^{L(U)}(\mu_i)(i = (0,1,2))$ can be directly calculated as

$$p_0^{L(U)}(\mu_i) = P_{0,A}^{L(U)}(\mu_i)P_{0,A}^{L(U)}(\mu_i), \tag{5}$$

$$p_1^{L(U)}(\mu_i) = P_{0,A}^{L(U)}(\mu_i)P_{1,B}^{L(U)}(\mu_i) + P_{1,A}^{L(U)}(\mu_i)P_{0,B}^{L(U)}(\mu_i), \tag{6}$$

$$p_2^{L(U)}(\mu_i) = P_{0,A}^{L(U)}(\mu_i)P_{2,B}^{L(U)}(\mu_i) + P_{2,A}^{L(U)}(\mu_i)P_{0,B}^{L(U)}(\mu_i) + P_{1,A}^{L(U)}(\mu_i)P_{1,B}^{L(U)}(\mu_i). \tag{7}$$

2.2. Security Analysis

In the SNS protocol, Z-data are generated from effective events when Alice (Bob) sends a signal state while Bob (Alice) does not. Therefore, the security of the SNS protocol is equivalent to that of the BB84 protocol with a decoy-state scheme. Equation (2) holds under asymptotic conditions. However, the key challenge lies in accurately estimating s_1^L, e_1^U. For X-data, when both communicating parties select decoy states of the same intensity, the output two-mode quantum state is given by $|\varphi\rangle = |\sqrt{\mu}e^{i\delta_A}\rangle \otimes |\sqrt{\mu}e^{i\delta_B}\rangle$, where μ represents the average photon number of the decoy state. Although the random phases δ_A and δ_B in X-data satisfy Equation (1), indicating that $\delta_A - \delta_B$ is not random, the value of $\delta_A + \delta_B$

remains random. We define a new variable $\delta_{\pm} = \delta_A \pm \delta_B$. Under this new variable, the output quantum state becomes [25]

$$|\varphi\rangle = |\sqrt{\mu}e^{i\frac{\delta_+ + \delta_-}{2}}\rangle \otimes |\sqrt{\mu}e^{\frac{\delta_+ - \delta_-}{2}}\rangle. \tag{8}$$

In Eve's view, the dual light field state can be regarded as a mixed state represented by $|\varphi\rangle$ due to the random selection of δ_+ over the interval $[0, 2\pi)$. Therefore, the SNS protocol confirms that after transmission through the channel, the dual light field state can be expressed as shown in Equation (9).

$$\rho_{AB} = \sum_k p_k |\psi_k\rangle\langle\psi_k|. \tag{9}$$

In Equation (9), $|\psi_k\rangle$ denotes the component of the joint state of the two optical fields containing a total of k photons, while p_k represents the probability of this joint state occurring. This indicates that the decoy-state method can be applied to estimate the count rate and bit error rate of the single-photon component based on the X-data. Specifically, this applies to partial signals corresponding to zero-, single-, and two-photon components, where k = 0, 1, or 2 can be expressed as the following equations.

$$|\psi_0\rangle = |0\rangle_A|0\rangle_B, p_0 = e^{-2\mu}, \tag{10}$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + e^{i\Delta}|1\rangle_A|0\rangle_B), p_1 = 2\mu e^{-2\mu}, \tag{11}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|2\rangle_B + 2e^{i\Delta}|1\rangle_A|1\rangle_B + e^{i2\Delta}|2\rangle_A|0\rangle_B), p_2 = 2\mu^2 e^{-2\mu}, \tag{12}$$

$$\Delta = \delta_A + \gamma_A - \delta_B - \gamma_B. \tag{13}$$

Under untrusted source conditions, as opposed to ideal light source conditions, each communicating party emits arbitrary quantum states as

$$\left|\psi_{A(B)}\right\rangle = \sum_{n=0}^{\infty} e^{in(\delta_{A(B)} + \gamma_{A(B)})} \sqrt{P_{n,A(B)}(\mu)}|n\rangle_{A(B)}. \tag{14}$$

Referring to the SNS protocol [25], a new variable $\delta_{\pm} = \delta_A \pm \delta_B$ is defined, which leads to Eve's observation that the joint state sent by the two communicating parties can be expressed as

$$\rho_{AB} = \int_0^{2\pi} P(|\psi_A\rangle \otimes |\psi_B\rangle) d\delta_+, \tag{15}$$

$P(|x\rangle) = |x\rangle\langle x|$ refers to the density operator. Calculating and normalizing Equation (15) yields the result.

$$\rho_{AB} = \sum_n p_n(\mu)|\psi_n\rangle\langle\psi_n|, \tag{16}$$

$$|\psi_n\rangle = \frac{1}{\sqrt{P_n(\mu)}} \sum_{k=0}^{n} \sqrt{P_{k,A}(\mu)P_{n-k,B}(\mu)}|k\rangle_A|n-k\rangle_B, \tag{17}$$

$$p_n(\mu) = \sum_{k=0}^{n} P_{k,A}(\mu)P_{n-k,B}(\mu). \tag{18}$$

Further analysis shows that when the light source conditions of both communicating parties are consistent,

$$P_{k,A}(\mu) = P_{k,B}(\mu) = P_k(\mu), \tag{19}$$

the single-photon component of ρ_{AB} can be expressed as

$$\left|\psi_1^{'}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B + e^{i\Delta}|1\rangle_A|0\rangle_B\right). \tag{20}$$

This means that the same results can be obtained as with ideal light sources even under untrusted light source conditions. Therefore, the security analysis method of the original SNS protocol remains valid. Under untrusted source conditions, the security of the protocol can still be guaranteed.

2.3. Parameters Estimation with UB

In the original SNS protocol, Alice (Bob) sends a coherent signal [25], where the average number of photons follows a Poisson distribution

$$P_{n,A}(\mu) = P_{n,B}(\mu) = P_n(\mu) = e^{-\mu}\frac{\mu^n}{n!}, \tag{21}$$

we can then calculate Equations (5)–(7) using Equation (21). However, under untrusted light conditions, the photon distribution no longer follows a Poisson distribution. Therefore, light source monitoring is required to estimate $p_0^{L(U)}(\mu_i)$, $p_1^{L(U)}(\mu_i)$ and $p_2^{L(U)}(\mu_i)$.

The light structure of the SNS protocol is similar to that of the MDI protocol with both protocols sharing similarities in phase and intensity modulation. The details of the SNS protocol, which is based on the UB monitoring scheme, are shown in Figure 1. The communicating parties estimate the probabilities of zero-, one-, and two-photon signals $P_{k,A}(\mu), P_{k,B}(\mu)(k = 0, 1, 2)$. Specifically, the monitoring parameter can be obtained through the UB light monitoring structure, which is the UB signal ratio, and it is denoted as Δ. Δ is expressed by the following inequality:

$$1 - \Delta \leq \sum_{N=N_{\min}}^{N_{\max}} P(N) \leq 1. \tag{22}$$

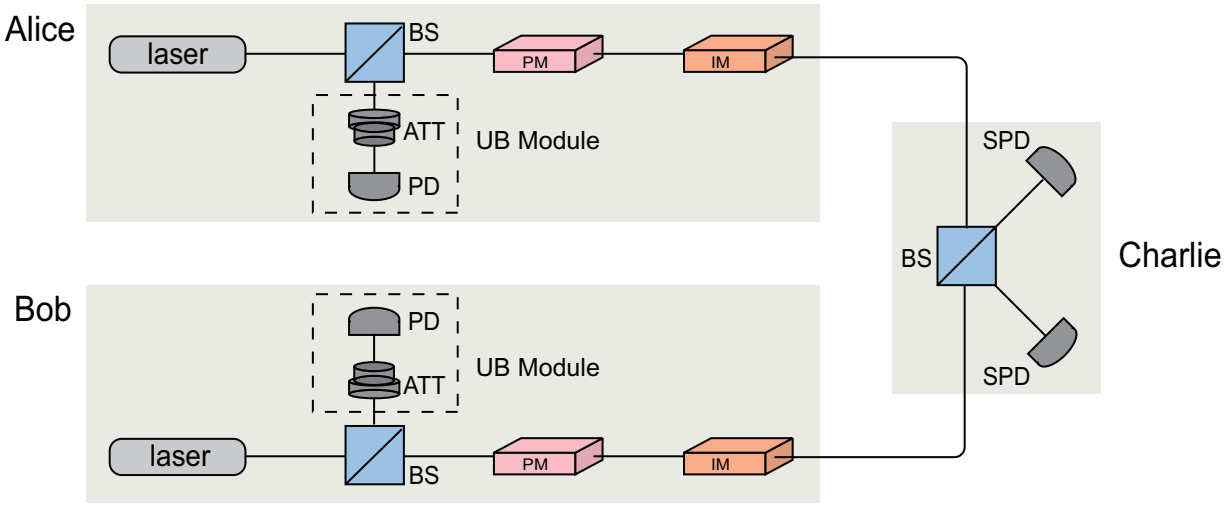

Figure 1. The structure of the sending-or-not-sending (SNS) protocol with an extra UB module in each of Alice's and Bob's parts. The UB module is composed of an attenuator (ATT) and a photon detector (PD).

The UB signal is defined as photons n_a and n_b, which are prepared by the communicating parties and located in the signal intervals $\left[N_{\min}^A, N_{\max}^A\right]$ and $\left[N_{\min}^B, N_{\max}^B\right]$, respectively. $1 - \Delta$ represents the probability that both communicating parties send UB signals. By

applying Equation (22), the probabilities of zero-, single-, and two-photon signals in the secure bit rate formula can be further estimated using the following key parameters

$$P_i^{\alpha} = \sum_{N=0}^{\infty} P(N) P_N^{\alpha}(i), (i \in \{0,1,2\}). \tag{23}$$

$P_N^{\alpha}(m)$ is the probability that the final signal after transmission contains m photons when the original signal has N photons with intensity α.

$$P_N^{\alpha}(m) = C_N^m \eta_{\alpha}^m (1-\eta_{\alpha})^{N-m}. \tag{24}$$

As a result, with the analysis shown in Appendix A, we can obtain the upper and lower bounds of P_i^{α}.

$$P_0^{\alpha} \geq (1-\Delta)(1-\eta_{\alpha})^{N_{\max}}, \tag{25}$$

$$P_0^{\alpha} \leq \Delta + (1-\Delta)(1-\eta_{\alpha})^{N_{\min}} + \Delta(1-\eta_{\alpha})^{N_{\max}+1}, \tag{26}$$

$$P_1^{\alpha} \geq \sum_{N=N_{\min}}^{N_{\max}} P(N) N_{\min} \eta_{\alpha} (1-\eta_{\alpha})^{N_{\min}-1} \geq (1-\Delta) N_{\min} \eta_{\alpha} (1-\eta_{\alpha})^{N_{\min}-1}, \tag{27}$$

$$\begin{aligned} P_1^{\alpha} \leq{}& \Delta(N_{\min}-1)\eta_{\alpha}(1-\eta_{\alpha})^{N_{\min}-2} + (1-\Delta)N_{\max}\eta_{\alpha}(1-\eta_{\alpha})^{N_{\max}-1} \\ &+ \Delta\widetilde{N}\eta_{\alpha}(1-\eta_{\alpha})^{\widetilde{N}-1}, \end{aligned} \tag{28}$$

$$P_2^{\alpha} \geq (1-\Delta)\frac{N_{\min}(N_{\min}-1)}{2}\eta_{\alpha}^2(1-\eta_{\alpha})^{N_{\min}-2}, \tag{29}$$

$$F_2^{\alpha} \leq \Delta C_{N_{\min-1}}^2 \eta_{\alpha}^2 (1-\eta_{\alpha})^{N_{\min}-3} + (1-\Delta) C_{N_{\max}}^2 \eta_{\alpha}^2 (1-\eta_{\alpha})^{N_{\max}-2} + \Delta C_{\overline{N}}^2 \eta_{\alpha}^2 (1-\eta_{\alpha})^{\overline{N}-2}. \tag{30}$$

The previous analysis precisely determines the upper and lower bounds of P_i^{α}. Furthermore, by substituting the results into Equations (3) and (4), the key parameters—the single photon response rate and bit error rate—can be estimated for the protocol's security analysis. Finally, the secure bit rate R is calculated using the formula in Equation (2).

3. Performance with Numerical Simulation

The key parameter in the secure bit rate formula for the UB light monitoring scheme is the UB signal proportion $1-\Delta$, which is determined by the actual light source signal characteristics and the UB signal interval $[N_{\min}, N_{\max}]$. Δ can be expressed as the following equation [45]

$$\Delta = G(\mu) = 1 - \frac{1}{2}\left[\operatorname{erf}\left(\frac{N_{\max}-\mu}{\sqrt{2\mu}}\right) - \operatorname{erf}\left(\frac{N_{\min}-\mu}{\sqrt{2\mu}}\right)\right], \tag{31}$$

when the light source is considered ideal, $u = \bar{N}$ and the Δ can be directly calculated.

However, in practical analysis, the laser device is affected by the working environment, and fluctuations in light intensity are commonly observed. To simulate the experimental environment, we introduce the light intensity fluctuation parameter σ_0 and set Δ as

$$\Delta = 1 - \int_{N_{min}}^{N_{max}} [1 - G(\mu)] P(\mu) d\mu, \tag{32}$$

$$P(\mu) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{(\mu-\mu_0)^2}{2\sigma^2}\right), \tag{33}$$

$$\sigma = \sigma_0 \times \bar{N}, \mu_0 = \bar{N}. \tag{34}$$

Other calculation parameters are similar to those in the original SNS [25,26] protocol. To accurately estimate the performance of the UB light monitoring scheme, it is necessary to select an appropriate light source signal range based on experimental conditions to determine the UB signal proportion, which is followed by the calculation of the ideal secure bit rate. To simulate the experimental environment, we select the average photon number $\bar{N} = 1 \times 10^7$, the light intensity fluctuation parameter $\sigma_0 = 1\%$ and the interval parameter $\delta = 0.043$. Additionally, the traversal interval is set to $[N_{min}, N_{max}] = [(1-\delta)N, (1+\delta)N]$ followed by performance simulation under these conditions.

Based on the parameter estimation results from the previous section, simulations of the SNS protocol using the UB monitoring scheme can be performed under untrusted source conditions. First, we perform a performance simulation of the SNS protocol using ideal experimental parameters, which are set to be the same as in Reference [25] and listed in Table 1. The simulation results are shown in Figure 2. They demonstrate that the protocol can achieve performance close to that of an ideal light source environment, even under untrusted source conditions, when the UB light source monitoring is introduced. Under the set monitoring conditions, the maximum secure transmission distance can reach 817.5 km, which is over 95% of the ideal light source environment.

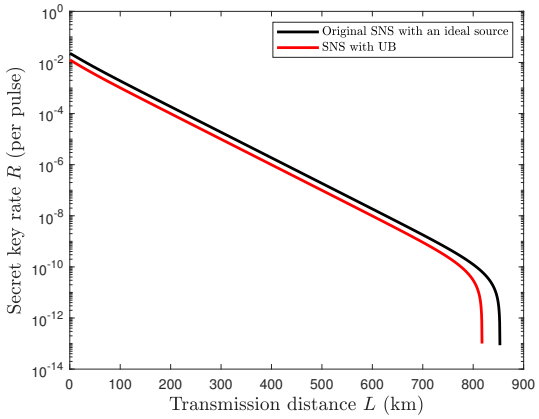

Figure 2. Performance diagram of SNS protocol based on UB monitoring solution under ideal parameters.

Table 1. Values of parameters used in simulation. α: the fiber loss coefficient (unit: dB/km); p_d: 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	p_d	η_D	e_{det}	f
0.2 dB/km	1×10^{-11}	0.8	1%	1.1

Furthermore, we can analyze the performance of this monitoring scheme under untrusted source conditions and actual simulation parameters. The simulation results are shown in Figure 3. To simulate a real-world QKD system, we also consider factors such as a high dark count rate and low detection efficiency. Additionally, factors such as fiber attenuation, inherent system errors, and non-ideal data coordination efficiency are also considered in a non-ideal environment. Finally, the experimental parameters are chosen based on Table 2. The simulation result shows that under untrusted source conditions, the maximum secure transmission of the SNS protocol based on the UB monitoring scheme can reach 490 km, which is over 92% of the ideal light source environment. According to this result, although combining the UB monitoring scheme requires sacrificing some signals outside the UB interval, the performance can still be maintained within an acceptable range under certain experimental conditions.

Table 2. Values of parameters used in simulation (set as in Refs. [24,46] for more practical conditions).

α	p_d	η_D	e_{det}	f
0.2 dB/km	1×10^{-8}	0.6	2%	1.15

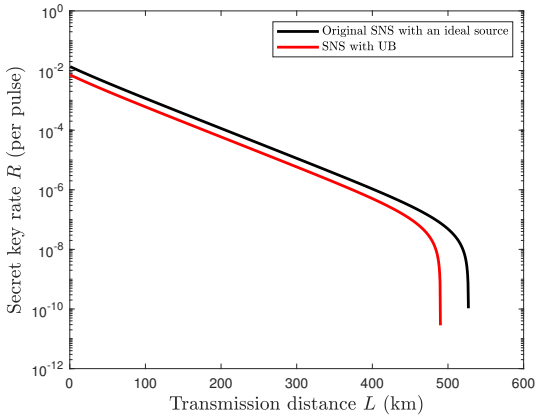

Figure 3. Performance diagram of SNS protocol based on UB monitoring solution under actual parameters.

4. Conclusions

Under untrusted source conditions, the primary factors to consider are the security of the dual light-field protocol as well as sufficient secure bit rate and transmission. In this paper, we introduce UB light monitoring into the SNS protocol. The introduction of UB light-source monitoring in the SNS protocol provides a novel and effective solution. By externally monitoring the light source signals of the communicating parties, following filtering and phase randomization, the proportion of UB signals with photon numbers within a specified interval $[N_{\min}, N_{\max}]$ can be determined. This allows for the accurate estimation of key parameters in the protocol's security bit rate formula, such as the probabilities of zero-photon, single-photon, and two-photon signals. Consequently, a compact lower bound for the security bit rate can be effectively determined. Furthermore, this scheme monitors the laser source signal before attenuation, bypassing the challenges of low detection efficiency and high costs commonly associated with single-photon detection for weak light monitoring.

The simulation analysis demonstrates that this scheme can achieve 817.5 km of secure transmission under ideal simulation parameters, which closely matches the transmission performance of an ideal light source environment. Under actual simulation parameters, the scheme can achieve 490 km of secure transmission, matching over 92% of the performance in an ideal light source environment. Compared to other protocol schemes, this scheme demonstrates better tolerance to light source fluctuations and offers significant advantages in transmission distance and secure bit rate.

Author Contributions: Conceptualization, J.H. and W.L.; methodology, J.H. and W.L.; validation, J.H. and Y.Q.; formal analysis, J.H., Y.Q. and W.L.; investigation, J.H. and W.L.; resources, Y.Q.; writing—original draft preparation, J.H.; writing—review and editing, J.H. and W.L.; visualization, J.H.; funding acquisition, Y.Q. 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 (62301177) and Guangxi Science and Technology Program (GuiKeAD21220107).

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

Appendix A. The Bounds Estimation of P_i^α

The attenuation coefficient η_α^m represents the total attenuation from the laser source to the output when the original signal contains m photons. Here, $\alpha = s, d$ denotes the signal and decoy states, respectively. η_α^m is given by the following equation

$$\eta_\alpha = \frac{\mu_\alpha}{\overline{N}} = \frac{2\mu_\alpha}{N_{\min} + N_{\max}}. \tag{A1}$$

The upper and lower bounds of $P_i^\alpha (i = 0, 1, 2)$ can be estimated theoretically. The elimination method is similar to the decoy scheme and can be used to scale the decay probability when $N \in [N_{\min}, N_{\max}]$. Firstly, $P_i^\alpha (i = 0, 1, 2)$ can be rewritten as

$$P_i^\alpha = \sum_{N=0}^{N_{\min}-1} P(N) P_N^\alpha(i) + \sum_{N=N_{\min}}^{N_{\max}} P(N) P_N^\alpha(i) + \sum_{N=N_{\max}+1}^{\infty} P(N) P_N^\alpha(i). \tag{A2}$$

Analyzing the upper and lower bounds of each component in Equation (A2)

$$\frac{C_{N+1}^i (1-\eta_\alpha)^{N+1}}{C_N^i (1-\eta_\alpha)^N} = \frac{N+1}{N+1-i}(1-\eta_\alpha) = \left(1 + \frac{i}{N+1-i}\right)(1-\eta_\alpha). \tag{A3}$$

When i = 0,

$$\frac{C_{N+1}^0 (1-\eta_\alpha)^{N+1}}{C_N^0 (1-\eta_\alpha)^N} < 1, \tag{A4}$$

$$P_{N_{\max}}^\alpha\left(0\right) \le P_N^\alpha\left(0\right) \le P_{N_{\min}}^\alpha\left(0\right). \tag{A5}$$

By substituting Equation (A5) into Equation (24), we obtain

$$P_0^\alpha \ge \sum_{N=N_{\min}}^{N_{\max}} P(N) P_N^\alpha(0) \ge \sum_{N=N_{\min}}^{N_{\max}} P(N) C_{N_{\max}}^0 \eta_\alpha^0 (1-\eta_\alpha)^{N_{\max}-0}, \tag{A6}$$

$$\begin{aligned} P_0^\alpha \le & \sum_{N=0}^{N_{\min}-1} P(N) + \sum_{N=N_{\min}}^{N_{\max}} P(N) C_{N_{\min}}^0 \eta_\alpha^0 (1-\eta_\alpha)^{N_{\min}-0} \\ & + \sum_{N=0}^{N_{\min}-1} P(N) C_{N_{\max}+1}^0 \eta_\alpha^0 (1-\eta_\alpha)^{N_{\max}+1}, \end{aligned} \tag{A7}$$

because

$$\sum_{N=N_{\min}}^{N_{\max}} P(N) C_{N_{\max}}^0 \eta_\alpha^0 (1-\eta_\alpha)^{N_{\max}-0} = \sum_{N=N_{\min}}^{N_{\max}} P(N)(1-\eta_\alpha)^{N_{\max}} \ge (1-\Delta)(1-\eta_\alpha)^{N_{\max}}, \tag{A8}$$

$$\begin{aligned} & \sum_{N=0}^{N_{\min}-1} P(N) + \sum_{N=N_{\min}}^{N_{\max}} P(N) C_{N_{\min}}^0 \eta_\alpha^0 (1-\eta_\alpha)^{N_{\min}-0} + \sum_{N=0}^{N_{\min}-1} P(N) C_{N_{\max}+1}^0 \eta_\alpha^0 (1-\eta_\alpha)^{N_{\max}+1} \\ & \le \Delta + (1-\Delta)(1-\eta_\alpha)^{N_{\min}} + \Delta(1-\eta_\alpha)^{N_{\max}+1}, \end{aligned} \tag{A9}$$

by substituting Equation (A8) and Equation (A9) into Equation (A6) and Equation (A7), respectively, we can obtain the upper and lower bounds of P_0^α:

$$P_0^\alpha \ge (1-\Delta)(1-\eta_\alpha)^{N_{\max}}, \tag{A10}$$

$$P_0^\alpha \le \Delta + (1-\Delta)(1-\eta_\alpha)^{N_{\min}} + \Delta(1-\eta_\alpha)^{N_{\max}+1}. \tag{A11}$$

Likewise, for Equation (A3), when i = 1,

$$\frac{C_{N+1}^{1}(1-\eta_\alpha)^{N+1}}{C_{N}^{1}(1-\eta_\alpha)^{N}} = \frac{N+1}{N}\left(1-\frac{2\mu_\alpha}{N_{\min}+N_{\max}}\right), \tag{A12}$$

it can be seen that Equation (A12) decreases with N. Here, we make it equal to 1,

$$\frac{N+1}{N}\left(1-\frac{2\mu_\alpha}{N_{\min}+N_{\max}}\right) = 1, \tag{A13}$$

we can determine the inflection point N of Equation (A12)

$$N = \widetilde{N} = \frac{N_{\min}+N_{\max}}{2\mu_\alpha} - 1. \tag{A14}$$

In a QKD system, it is typically set that $\mu_\alpha < 1$, which implies that $\widetilde{N} > N_{\max}$. Based on the above result, the upper and lower bounds of P_1^α can be calculated.

$$P_1^\alpha \geq \sum_{N=N_{\min}}^{N_{\max}} P(N)P_N^\alpha(1) \geq \sum_{N=N_{\min}}^{N_{\max}} P(N)C_{N_{\min}}^{-1}\eta_\alpha^1(1-\eta_\alpha)^{N_{\min}-1}, \tag{A15}$$

$$\begin{aligned} P_1^\alpha \leq & \sum_{N=0}^{N_{\min}-1} P(N)P_N^\alpha(1) + \sum_{N=N_{\min}}^{N_{\max}} P(N)C_{N_{\max}}^{1}\eta_\alpha^1(1-\eta_\alpha)^{N_{\max}-1} \\ & + \sum_{N=N_{\max}+1}^{\infty} P(N)P_N^\alpha(1). \end{aligned} \tag{A16}$$

It should be noted that

$$\sum_{N=N_{\min}}^{N_{\max}} P(N) = 1-\Delta. \tag{A17}$$

To monitor the observable parameters, we can further simplify the upper and lower bounds of P_1^α:

$$P_1^\alpha \geq \sum_{N=N_{\min}}^{N_{\max}} P(N)N_{\min}\eta_\alpha(1-\eta_\alpha)^{N_{\min}-1} \geq (1-\Delta)N_{\min}\eta_\alpha(1-\eta_\alpha)^{N_{\min}-1}, \tag{A18}$$

$$\begin{aligned} P_1^\alpha \leq & \Delta(N_{\min}-1)\eta_\alpha(1-\eta_\alpha)^{N_{\min}-2} + (1-\Delta)N_{\max}\eta_\alpha(1-\eta_\alpha)^{N_{\max}-1} \\ & + \Delta\widetilde{N}\eta_\alpha(1-\eta_\alpha)^{\widetilde{N}-1}. \end{aligned} \tag{A19}$$

Finally, when i = 2, Equation (A3) can be written as

$$\frac{C_{N+1}^{1}(1-\eta_\alpha)^{N+1}}{C_{N}^{1}(1-\eta_\alpha)^{N}} = \frac{N+1}{N-1}\left(1-\frac{2\mu_\alpha}{N_{\min}+N_{\max}}\right), \tag{A20}$$

similarly, the inflection point can be calculated as

$$\frac{N+1}{N}\left(1-\frac{2\mu_\alpha}{N_{\min}+N_{\max}}\right) = 1, \tag{A21}$$

thus, we obtain the following equation

$$\widetilde{\widetilde{N}} = \frac{N_{\min}+N_{\max}}{\mu_\alpha} - 1. \tag{A22}$$

Similarly, since $\mu_\alpha < 1$, it follows that $\widetilde{\widetilde{N}} > N_{\max}$. Based on this, we can determine the upper and lower bounds of P_2^α as follows

$$\begin{aligned} P_2^\alpha &\geq \sum_{N=N_{\min}}^{N_{\max}} P(N) P_N^\alpha(2) \geq \sum_{N=N_{\min}}^{N_{\max}} P(N) C_{N_{\min}}^2 \eta_\alpha^2 (1-\eta_\alpha)^{N_{\min}-2} \\ &= \sum_{N=N_{\min}}^{N_{\max}} P(N) \frac{N_{\min}(N_{\min}-1)}{2} \eta_\alpha^2 (1-\eta_\alpha)^{N_{\min}-2} \\ &\geq (1-\Delta) \frac{N_{\min}(N_{\min}-1)}{2} \eta_\alpha^2 (1-\eta_\alpha)^{N_{\min}-2}, \end{aligned} \tag{A23}$$

$$\begin{aligned} F_2^\alpha &\leq \sum_{N=0}^{N_{\min}-1} P(N) P_N^\alpha(2) + \sum_{N=N_{\min}}^{N_{\max}} P(N) C_{N_{\max}}^2 \eta_\alpha^2 (1-\eta_\alpha)^{N_{\max}-2} + \sum_{N=N_{\max}+1}^{\infty} P(N) P_N^\alpha(2) \\ &\leq \Delta C_{N_{\min-1}}^2 \eta_\alpha^2 (1-\eta_\alpha)^{N_{\min}-3} + (1-\Delta) C_{N_{\max}}^2 \eta_\alpha^2 (1-\eta_\alpha)^{N_{\max}-2} + \Delta C_{\overline{N}}^2 \eta_\alpha^2 (1-\eta_\alpha)^{\overline{N}-2}. \end{aligned} \tag{A24}$$

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
2. Bennett, C.H.; Brassard, G.; Mermin, N.D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **1992**, *68*, 557. [CrossRef] [PubMed]
3. Scarani, V.; Acin, A.; Ribordy, G.; Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **2004**, *92*, 057901. [CrossRef]
4. Inoue, K.; Waks, E.; Yamamoto, Y. Differential phase shift quantum key distribution. *Phys. Rev. Lett.* **2002**, *89*, 037902. [CrossRef] [PubMed]
5. Bruß, D. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **1998**, *81*, 3018. [CrossRef]
6. Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **1992**, *5*, 3–28. [CrossRef]
7. Bechmann-Pasquinucci, H.; Tittel, W. Quantum cryptography using larger alphabets. *Phys. Rev. A* **2000**, *61*, 062308. [CrossRef]
8. Cerf, N.J.; Bourennane, M.; Karlsson, A.; Gisin, N. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.* **2002**, *88*, 127902. [CrossRef]
9. Mower, J.; Zhang, Z.; Desjardins, P.; Lee, C.; Shapiro, J.H.; Englund, D. High-dimensional quantum key distribution using dispersive optics. *Phys. Rev. A* **2013**, *87*, 062322. [CrossRef]
10. Liu, J.; Lin, Z.; Liu, D.; Feng, X.; Liu, F.; Cui, K.; Zhang, W. High-dimensional quantum key distribution using energy-time entanglement over 242 km partially deployed fiber. *Quantum Sci. Technol.* **2024**, *9*, 015003. [CrossRef]
11. Zahidy, M.; Ribezzo, D.; De Lazzari, C.; Vagniluca, I.; Biagi, N.; Müller, R.; Bacco, D. Practical high-dimensional quantum key distribution protocol over deployed multicore fiber. *Nat. Commun.* **2024**, *15*, 1651. [CrossRef] [PubMed]
12. Sekga, C.; Mafu, M.; Senekane, M. High-dimensional quantum key distribution implemented with biphotons. *Sci. Rep.* **2023**, *13*, 1229. [CrossRef]
13. Ding, Y.; Bacco, D.; Dalgaard, K.; Cai, X.; Zhou, X.; Rottwitt, K.; Oxenløwe, L.K. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *npj Quantum Inf.* **2017**, *3*, 25. [CrossRef]
14. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **2000**, *61*, 052304. [CrossRef]
15. Makarov, V.; Hjelme, D.R. Faked states attack on quantum cryptosystems. *J. Mod. Opt.* **2005**, *52*, 691–705. [CrossRef]
16. Qi, B.; Fung, C.H.F.; Lo, H.K.; Ma, X. Time-shift attack in practical quantum cryptosystems. *arXiv* **2005**, arXiv:quant-ph/0512080. [CrossRef]
17. Wei, K.; Liu, H.; Ma, H.; Yang, X.; Zhang, Y.; Sun, Y.; Xiao, J.; Ji, Y. Feasible attack on detector-device-independent quantum key distribution. *Sci. Rep.* **2017**, *7*, 449. [CrossRef]
18. Gottesman, D.; Lo, H.K.; Lütkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. In Proceedings of the International Symposium on Information Theory (ISIT 2004), Chicago, IL, USA, 27 June–2 July 2004; Volume 136.
19. Hwang, W.-Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef]
20. 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]
21. 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]

22. 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]
23. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
24. 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]
25. 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]
26. 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*, 3080. [CrossRef]
27. 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]
28. 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]
29. Peng, Q.; Chen, J.P.; Xing, T.; Wang, D.; Wang, Y.; Liu, Y.; Huang, A. Practical security of twin-field quantum key distribution with optical phase-locked loop under wavelength-switching attack. *npj Quantum Inf.* **2025**, *11*, 7. [CrossRef]
30. Sun, M.S.; Zhang, C.H.; Ma, X.; Zhou, X.Y.; Wang, Q. Sending-or-not-sending twin-field quantum key distribution with measurement imperfections. *IEEE Commun. Lett.* **2022**, *26*, 2004–2008. [CrossRef]
31. 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]
32. Liu, H.; Jiang, C.; Zhu, H.T.; Zou, M.; Yu, Z.W.; Hu, X.L.; Xu, H.; Ma, S.; Han, Z.; Chen, J.-P.; et al. Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km. *Phys. Rev. Lett.* **2021**, *126*, 250502. [CrossRef]
33. Liu, Y.; Zhang, W.J.; Jiang, C.; Chen, J.P.; Zhang, C.; Pan, W.X.; Ma, D.; Dong, H.; Xiong, J.-M.; Zhang, C.-J.; et al. Experimental twin-field quantum key distribution over 1000 km fiber distance. *Phys. Rev. Lett.* **2023**, *130*, 210801. [CrossRef]
34. Liu, Y.; Zhang, W.J.; Jiang, C.; Chen, J.P.; Ma, D.; Zhang, C.; Pan, J.W. 1002 km twin-field quantum key distribution with finite-key analysis. *Quantum Front.* **2023**, *2*, 16. [CrossRef]
35. Shan, Y.G.; Zhou, Y.; Yin, Z.Q.; Wang, S.; Chen, W.; He, D.Y.; Han, Z.F. Sending-or-not-sending quantum key distribution with phase postselection. *Phys. Rev. Appl.* **2024**, *22*, 024056. [CrossRef]
36. Qiao, Y.; Chen, Z.; Zhang, Y.; Xu, B.; Guo, H. Sending-or-not-sending twin-field quantum key distribution with light source monitoring. *Entropy* **2019**, *22*, 36. [CrossRef]
37. Lu, Y.F.; Wang, Y.; Jiang, M.S.; Liu, F.; Zhang, X.X.; Bao, W.S. Finite-key analysis of sending-or-not-sending twin-field quantum key distribution with intensity fluctuations. *Quantum Inf. Process.* **2021**, *20*, 135. [CrossRef]
38. 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*, 320. [CrossRef]
39. 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. [CrossRef]
40. 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]
41. 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]
42. Hu, X.L.; Jiang, C.; Yu, Z.W.; Wang, X.B. Sending-or-not-sending twin-field quantum key distribution with imperfect vacuum sources. *New J. Phys.* **2022**, *24*, 063014. [CrossRef]
43. Wen, K.; Fei, L.; Wan, Z.A.; Wu, X.Y.; Li, H.T.; Peng, H.; Li, Y.P. Intensity fluctuation analysis for sending or not sending twin field quantum key distribution. *Proc. SPIE* **2023**, *12617*, 1390–1397.
44. Sun, M.S.; Wang, W.L.; Zhou, X.Y.; Zhang, C.H.; Wang, Q. Source monitoring twin-field quantum key distribution assisted with Hong-Ou-Mandel interference. *Phys. Rev. Res.* **2023**, *5*, 043179. [CrossRef]
45. Zhao, Y.; Qi, B.; Lo, H.K. Quantum key distribution with an unknown and untrusted source. *Phys. Rev. A* **2008**, *77*, 052327. [CrossRef]
46. Park, J.; Lee, J.; Heo, J. Improved statistical fluctuation analysis for twin-field quantum key distribution. *Quantum Inf. Process.* **2021**, *20*, 127. [CrossRef]