applied sciences

MDPI

Article

Finite-Key Analysis of 1-Decoy Method Quantum Key Distribution with Intensity Fluctuation

Chun Zhou [1,2,†], Yu Zhou [1,2,†], Yangbin Xu [1,2], Yang Wang [1,2,3], Yifei Lu [1,2], Musheng Jiang [1,2], Xiaoxu Zhang [1,2] and Wansu Bao [1,2,*]

1 Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou 450001, China; zc@qiclab.cn (C.Z.); zy@qiclab.cn (Y.Z.); xyb@qiclab.cn (Y.X.); wy@qiclab.cn (Y.W.); lyf@qiclab.cn (Y.L.); jms@qiclab.cn (M.J.); zxx@qiclab.cn (X.Z.)
2 Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China
3 National Laboratory of Solid State Microstructures, School of Physics and Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China
* Correspondence: bws@qiclab.cn
† These authors contributed equally to this work.

Abstract: The decoy state quantum key distribution (QKD) protocol is proven to be an effective strategy against the photon number splitting attack. It was shown that the 1-decoy state protocol, easier to implement in the practical QKD system, outperforms the 2-decoy state protocol for block sizes of up to 10^8 bits. How intensity fluctuations influence the performance of the 1-decoy state protocol with finite resources remains a pending issue. In this paper, we present a finite-key analysis of the 1-decoy state protocol with intensity fluctuations and obtain the secret key rate formula about intensity fluctuations. Our numerical simulation results show that the stronger the intensity fluctuations, the lower the secret key rate for a small data block size of a few bits. Our research can provide theoretical implications for the selection of data size in the QKD system with intensity fluctuations.

Keywords: 1-decoy; finite key; intensity fluctuation; Azuma inequality

Citation: Zhou, C.; Zhou, Y.; Xu, Y.; Wang, Y.; Lu, Y.; Jiang, M.; Zhang, X.; Bao, W. Finite-Key Analysis of 1-Decoy Method Quantum Key Distribution with Intensity Fluctuation. *Appl. Sci.* **2022**, *12*, 4709. https://doi.org/10.3390/app12094709

Academic Editors: Durdu Guney and David Petrosyan

Received: 18 March 2022
Accepted: 6 May 2022
Published: 7 May 2022

1. Introduction

Quantum key distribution (QKD) [1], whose security is guaranteed by the fundamental quantum mechanics, has been developed for nearly four decades. Its secure transmission distance has grown from 32 cm in a free space channel to hundreds of kilometers in a low-loss fiber channel [2,3]. In particular, QKD based on single photon states and quantum entanglement states between minus satellite and its ground station has been successfully demonstrated [4], implying the feasibility of space-based QKD. However, due to the intrinsic imperfections of realizing devices, quantum hacking attacks [5–8], based on device loopholes, bring great threats to the practical security of QKD. For example, the weak coherent source, usually used as a candidate of the true single-photon source, is vulnerable to the photon number splitting (PNS) [9–11] attack raised from multi-photon events.

Fortunately, the decoy state method proposed by Hwang [12] has been proven to be one of the most effective countermeasures against PNS attacks. Although the original decoy state method with an infinite number of intensities provides the best performance with optimal parameter estimation, its practical versions with a finite number of intensities [13–15] are shown to be effective enough to meet the usage requirements of real QKD systems. When taking the statistical fluctuation resulting from a finite-length data size into account, how the intensity fluctuations influence the security bounds of the QKD protocol remains to be deeply investigated, and some important results [16–20] have been obtained to answer this question. The 2-decoy state method outperforms the 1-decoy state method in the asymptotic case of infinite key length. However, when we turn to a practical data

block size, the results [21] indicate the 1-decoy state method is more advantageous than the 2-decoy state method by conducting a rigorous finite-key analysis using Hoeffding's inequality [22].

Many efforts have been made to improve the finite-key security bound by considering the statistical characteristics such as the Hoeffding's inequality, the Chernoff bound [23] and the Improved-Chernoff bound [24], which assume that the former event, current event and later event are independently related. However, in real-life QKD setups, since the intensities of the emitting signals from the photon source are not always steady, the counting events before and later gathered in the measurement setups may be related to each other [25]. Thus, the previous finite-key analysis methods are not suitable for these event-dependent scenarios. Then, it is necessary to find an appropriate statistical model to handle the dependent events and renew the upper security bound by taking intensity fluctuations into consideration. Otherwise, the eavesdropper (Eve) can acquire more secret information if one does not refresh the security bound. For different protocols, much work [26–28] has been acquired to relax the assumption that Alice can control the intensities of light sources with great accuracy. In particular, Wang et al. [18] studied the effects of both intensity fluctuations and classical statistical fluctuations for the 2-decoy state method with dependent events.

In this paper, we turn to the 1-decoy state method and re-examine its finite-key bound by taking both intensity fluctuations and dependent events into account. We obtain a secret key rate of the 1-decoy state method with different data sizes and different intensity fluctuations. Numerical simulations indicate that, as with the 2-decoy state method, intensity fluctuations have non-negligible effects on the performance of the 1-decoy state method. Most importantly, for the 1-decoy state method, the security bound with a small data size is more sensitive to intensity fluctuations than that with a large data size. This paper is organized as follows. Section 2 conducts a finite-key analysis for the 1-decoy state method with intensity fluctuations and dependent events. In Section 3, the simulation results are shown, and a conclusion is obtained in Section 4.

2. The Finite-Key Analysis of 1-Decoy with Intensity Fluctuations

The 1-decoy method was presented as a simpler method with only two intensities, i.e., a signal and a decoy state, denoted as μ_1 and μ_2, respectively. In practical scenarios, the intensity fluctuations are usually caused by imperfections of the laser and the intensity modulators. Therefore, it is too difficult to use a specific analytical method to describe the intensities' fluctuations, but the range of the intensity can be assumed as $\mu_i \in [{\mu_i}^-, {\mu_i}^+], \mu_i \in \{\mu_1, \mu_2\}$. Furthermore, we can characterize intensity fluctuations by ${\mu_i}^- = (1-\delta_\mu)\mu_i$ and ${\mu_i}^+ = (1+\delta_\mu)\mu_i$, where the parameter δ_μ is used to quantify the degree of intensity fluctuation. Once the source is determined, the δ_μ can be regarded as constant. For each intensity, the probability that the light source produces the n-photon states is $p_{n|\mu_i}$, which can be written as [18]

$$\frac{e^{-{\mu_i}^+}({\mu_i}^-)^n}{n!} \leq p_{n|\mu_i} = \frac{e^{-\mu_i}{\mu_i}^n}{n!} \leq \frac{e^{-{\mu_i}^-}({\mu_i}^+)^n}{n!}. \tag{1}$$

When the intensity fluctuations are not considered, the total probability that Alice sends n-photon states can be expressed as $\tau_n = \sum_{\mu_i \in \{\mu_1,\mu_2\}} p_{\mu_i} e^{-\mu_i} {\mu_i}^n / n!$. However, intensity fluctuations of modulation will affect the probability τ_n, and we can obtain the range of the τ_n as follows:

$$\tau_n^- = \sum_{\mu_i \in \{\mu_1,\mu_2\}} p_{\mu_i} e^{-{\mu_i}^+} ({\mu_i}^-)^n / n! \leq \tau_n \leq \sum_{\mu_i \in \{\mu_1,\mu_2\}} p_{\mu_i} e^{-{\mu_i}^-} ({\mu_i}^+)^n / n! = \tau_n^+. \tag{2}$$

We set p_{μ_i} to represent the probability of Alice choosing intensity μ_i and the probability $p_{\mu_i|n}$ denotes the probability of n-photon coming from specific intensity μ_i in the total n-photon detection events.

$$\frac{p_{\mu_i} e^{-{\mu_i}^+} ({\mu_i}^-)^n}{\tau_n^+ n!} \leq p_{\mu_i|n} = \frac{p_{\mu_i} e^{-\mu_i} {\mu_i}^n}{\tau_n n!} \leq \frac{p_{\mu_i} e^{-{\mu_i}^-} ({\mu_i}^+)^n}{\tau_n^- n!}. \tag{3}$$

Let N_α be the total number observed by Bob on $\alpha \in \{Z, X\}$ basis. The $s_{\alpha,n}$ are the total detections observed by Bob in which Alice sent n-photon states on $\alpha \in \{Z, X\}$ basis. The number of detection events with a specific intensity μ_i should be N^*_{α,μ_i} and the N_{α,μ_i} is the expectation of the amount of detection events. Then, we have

$$N_\alpha = \sum_{\mu_i \in \{\mu_1, \mu_2\}} N_{\alpha,\mu_i} = \sum_{n=0}^{\infty} s_{\alpha,n}. \tag{4}$$

In this paper, the effects of statistical fluctuations and intensity fluctuations are taken into account concurrently. We use the concentration inequality to describe the relationship between expected and observed values. Significantly, the intensity fluctuations will destroy the independence between response events. Therefore, we should use Azuma's inequality [20], which holds with dependent random samples, to characterize the relation between the expected values and the observed values. The observed values N^*_{α,μ_i} shall be deviated from the expected values N_{α,μ_i} by

$$\mid N_{\alpha,\mu_i} - N^*_{\alpha,\mu_i} \mid \leq \delta_A(N_\alpha, \varepsilon_{A1}), \tag{5}$$

with the probability of at least $1 - 2\varepsilon_{A1}$, where the $\delta_A(x, y) = \sqrt{2xln(\frac{1}{y})}$. Moreover, $N_\alpha = \sum_{\mu_i \in \{\mu_1, \mu_2\}} N_{\alpha,\mu_i}$ is the total number of events when Bob and Alice both choose α basis. Simultaneously, M^*_{α,μ_i}, the number of errors observed on α basis with the intensity μ_i, can be estimated with the same method. One can obtain the following relation:

$$\mid M_{\alpha,\mu_i} - M^*_{\alpha,\mu_i} \mid \leq \delta_A(M_\alpha, \varepsilon_{A2}), \tag{6}$$

with the probability at least $1 - 2\varepsilon_{A2}$. Moreover, $M_\alpha = \sum_{\mu_i \in \{\mu_1, \mu_2\}} M_{\alpha,\mu_i}$ is the total number of errors in which Alice sent states on α basis. Thence, we can bound N^*_{α,μ_i} and M_{α,μ_i} for a given intensity $\mu_i \in \{\mu_1, \mu_2\}$, respectively, as follows:

$$N^{*L}_{\alpha,\mu_i} = N_{\alpha,\mu_i} - \delta_A(N_\alpha, \varepsilon_{A1}) \leq N^*_{\alpha,\mu_i} \leq N_{\alpha,\mu_i} + \delta_A(N_\alpha, \varepsilon_{A1}) = N^{*U}_{\alpha,\mu_i}, \tag{7}$$

$$M^{*L}_{\alpha,\mu_i} = M_{\alpha,\mu_i} - \delta_A(M_\alpha, \varepsilon_{A2}) \leq M^*_{\alpha,\mu_i} \leq M_{\alpha,\mu_i} + \delta_A(M_\alpha, \varepsilon_{A2}) = M^{*U}_{\alpha,\mu_i}. \tag{8}$$

After error correction and privacy amplification, the upper bound on the secret key length of the 1-decoy can be derived as [21]:

$$l \geq s^L_{Z,0} + s^L_{Z,1}(1 - h(\phi^U_Z)) - \lambda_{EC} - 6log(19/\varepsilon_{sec}) - log(2/\varepsilon_{cor}). \tag{9}$$

where λ_{EC} is the number of bits leaked during the error correction step; ε_{sec} and ε_{cor} are the secrecy and correctness parameters.

According to Equations (1) and (4), we can obtain the detailed expression of the boundary of N^*_{α,μ_i}

$$p_{\mu_i} \sum_{n=0}^{\infty} \frac{e^{-{\mu_i}^+} ({\mu_i}^-)^n}{\tau_n^+ n!} s_{\alpha,n} \leq N^*_{\alpha,\mu_i} \leq p_{\mu_i} \sum_{n=0}^{\infty} \frac{e^{-\mu^-} ({\mu_i}^+)^n}{\tau_n^- n!} s_{\alpha,n}. \tag{10}$$

Thence, we can obtain the following bounds:

$$\frac{e^{\mu_1^+} N^*_{Z,\mu_1}}{p_{\mu_1}} \geq \frac{s_{Z,0}}{\tau_0^+} + \frac{\mu_1^- s_{Z,1}}{\tau_1^+} + \sum_{n=2}^{\infty} \frac{(\mu_1^-)^n}{\tau_n^+ n!} s_{Z,n}, \tag{11}$$

$$\frac{e^{\mu_2^-} N^*_{Z,\mu_2}}{p_{\mu_2}} \leq \frac{s_{Z,0}}{\tau_0^+} + \frac{\mu_2^+ s_{Z,1}}{\tau_1^+} + \sum_{n=2}^{\infty} \frac{(\mu_2^+)^n}{\tau_n^+ n!} s_{Z,n}. \tag{12}$$

By adding Equations (11) and (12), we can obtain

$$\frac{e^{\mu_1^+} N^*_{Z,\mu_1}}{p_{\mu_1}} - \frac{e^{\mu_2^-} N^*_{Z,\mu_2}}{p_{\mu_2}} \geq \frac{(\mu_1^- - \mu_2^+) s_{Z,1}}{\tau_1^+} + \sum_{n=2}^{\infty} \frac{(\mu_1^-)^n - (\mu_2^+)^n}{\tau_n^+ n!} s_{Z,n}. \tag{13}$$

Even if the μ_1^- is the lower of the μ_1 and the μ_2^+ is the upper of the μ_2, the relationship $\mu_1^- > \mu_2^+$ still holds. Therefore, we can obtain

$$(\mu_1^-)^n - (\mu_2^+)^n \geq (\mu_2^+)^{n-2}((\mu_1^-)^2 - (\mu_2^+)^2). \tag{14}$$

Therefore, we can obtain

$$\begin{aligned} \frac{e^{\mu_1^+} N^*_{Z,\mu_1}}{p_{\mu_1}} - \frac{e^{\mu_2^-} N^*_{Z,\mu_2}}{p_{\mu_2}} \geq & \frac{((\mu_1^-)^2 - (\mu_2^+)^2)}{(\mu_2^+)^2} \left(\frac{e^{\mu_2^+} N^*_{Z,\mu_2}}{p_{\mu_2}} - \frac{s_{Z,0}}{\tau_0^-}\right) \\ & + \left(\frac{(\mu_1^- - \mu_2^+)}{\tau_1^+} - \frac{(\mu_1^-)^2 - (\mu_2^+)^2}{\mu_2^+ \tau_1^-}\right) s_{Z,1}. \end{aligned} \tag{15}$$

It is easy to isolate $s_{Z,1}$ from Equation (15):

$$\begin{aligned} s_{Z,1} \geq s^L_{Z,1} = & \frac{\tau_1^+ \tau_1^- \mu_2^+}{\mu_1^-(\mu_2^+ \tau_1^- - \mu_1^- \tau_1^+) + (\mu_2^+)^2(\tau_1^+ - \tau_1^-)} \left(\frac{e^{\mu_1^+} N^*_{Z,\mu_1}}{p_{\mu_1}} - \frac{e^{\mu_2^-} N^*_{Z,\mu_2}}{p_{\mu_2}}\right. \\ & \left. - \frac{((\mu_1^-)^2 - (\mu_2^+)^2)}{(\mu_2^+)^2} \left(\frac{e^{\mu_2^+} N^*_{Z,\mu_2}}{p_{\mu_2}} - \frac{s_{Z,0}}{\tau_0^-}\right)\right). \end{aligned} \tag{16}$$

In the 2-decoy method, three intensities (i.e., signal states, weak states and vacuum states) are needed to bound the vacuum events. For the 1-decoy method, there are two approaches to obtain the upper bound of the vacuum events. In this paper, we choose the latter, which provides the best secret key rate [15]. Let $m_{\alpha,n}$ be the number of errors detected at Bob's side when Alice sent n-photon states. We can obtain the upper bound by considering only the errors relative to the 1-decoy state:

$$M^*_{Z,\mu_i} = \sum_{n=0}^{\infty} p_{\mu_i|n} m_{Z,n} = \sum_{n=0}^{\infty} \frac{p_{\mu_i} e^{-\mu_i} {\mu_i}^n}{\tau_n n!} m_{Z,n} \geq \frac{p_{\mu_i} e^{-\mu_i} m_{Z,0}}{\tau_0} \geq \frac{p_{\mu_i} e^{-\mu_i{}^+} m_{Z,0}}{\tau_0^+}. \tag{17}$$

Therefore, we can obtain the upper bound of $m_{Z,0}$,

$$m_{Z,0} \leq \frac{\tau_0^+ e^{\mu_i{}^+} M^*_{Z,\mu_i}}{p_{\mu_i}} = g(\mu_i). \tag{18}$$

Since there are two intensities in the 1-decoy method, we can obtain a tighter upper bound as

$$m_{Z,0} \leq min(g(\mu_1), g(\mu_2)) = m^U_{Z,0}. \tag{19}$$

As the detectors respond to the vacuum events ($s_{Z,0}$) randomly, no information can be extracted from these events by Eve, and Bob also has only 50% probability of correct detection. Therefore, the expectation value of $m_{Z,0}$ should be half of the corresponding total events:

$$\frac{m_{Z,0}}{s_{Z,0}} = \frac{1}{2}. \tag{20}$$

In this way, we have the relation:

$$s_{Z,0} \leq s_{Z,0}^{U} = 2(m_{Z,0} + \delta_A(N_Z, \varepsilon_{A1})). \tag{21}$$

Therefore, combined with finite-key analysis, we can obtain the lower bound of $s_{Z,1}$

$$\begin{aligned} s_{Z,1} \geq \frac{\tau_1^+ \tau_1^- \mu_2^+}{\mu_1^-(\mu_2^+\tau_1^- - \mu_1^-\tau_1^+) + (\mu_2^+)^2(\tau_1^+ - \tau_1^-)}\Big(&\frac{e^{\mu_1^+} N_{Z,\mu_1}^{*U}}{p_{\mu_1}} - \frac{e^{\mu_2^-} N_{Z,\mu_2}^{*L}}{p_{\mu_2}} \\ &- \frac{((\mu_1^-)^2 - (\mu_2^+)^2)}{(\mu_2^+)^2}\Big(\frac{e^{\mu_2^+} N_{Z,\mu_2}^{*L}}{p_{\mu_2}} - \frac{s_{Z,0}^{U}}{\tau_0^-}\Big)\Big). \end{aligned} \tag{22}$$

By multiplying Equation (11) by μ_2^+ and Equation (12) by $-\mu_1^-$ and adding two inequalities, we can obtain

$$\begin{aligned} \frac{\mu_2^+ e^{\mu_1^+} N_{Z,\mu_1}^*}{p_{\mu_1}} - \frac{\mu_1^- e^{\mu_2^-} N_{Z,\mu_2}^*}{p_{\mu_2}} &\geq \frac{(\mu_2^+ - \mu_1^-)s_{Z,0}}{\tau_0} + \mu_2^+\mu_1^- \sum_{n=2}^{\infty} \frac{\left((\mu_1^-)^{n-1} - (\mu_2^+)^{n-1}\right)s_{Z,n}}{\tau_n n!} \\ &\geq \frac{(\mu_2^+ - \mu_1^-)s_{Z,0}}{\tau_0}. \end{aligned} \tag{23}$$

Since $\mu_1^- \geq \mu_2^+$, we can obtain

$$s_{Z,0} \geq s_{Z,0}^{L} = \frac{\tau_0^-}{\mu_2^+ - \mu_1^-}\Big(\frac{\mu_2^+ e^{\mu_1^+} N_{Z,\mu_1}^{*U}}{p_{\mu_1}} - \frac{\mu_1^- e^{\mu_2^-} N_{Z,\mu_2}^{*L}}{p_{\mu_2}}\Big). \tag{24}$$

Then, we need to estimate the phase error in the Z basis by following formula [21,29]:

$$\phi_Z := \frac{c_{Z,1}}{s_{Z,1}} \leq \frac{m_{X,1}^{U}}{s_{X,1}^{L}} + f\left(\varepsilon_{sec}, \frac{m_{X,1}^{U}}{s_{X,1}^{L}}, s_{Z,1}^{L}, s_{X,1}^{L}\right), \tag{25}$$

$$f(a,b,c,d) = \sqrt{\frac{(c+d)(1-b)b}{cdln2}} log_2\Big(\frac{(c+d)21^2}{cd(1-b)ba^2}\Big), \tag{26}$$

where $c_{Z,1}$ is the number of phase errors in the single-photon events when in the Z basis. Here, we estimate the phase error under Z basis by the bit error under X basis.

For $s_{X,1}^{L}$, we can use the same method as in $s_{Z,1}$ for calculation. In addition, $m_{X,1}$ can be bounded as in the following formulas. Similarly to the previous case, the M_{X,μ_i}^* can be described as:

$$p_{\mu_i} \sum_{n=0}^{\infty} \frac{e^{-\mu_i^+(\mu_i^-)^n} m_{X,n}}{\tau_n^+ n!} \leq M_{X,\mu_i}^* \leq p_{\mu_i} \sum_{n=0}^{\infty} \frac{e^{-\mu_i^-(\mu_i^+)^n} m_{X,n}}{\tau_n^- n!}. \tag{27}$$

For the specific intensity, there are

$$\frac{e^{\mu_2^-} M_{X,\mu_2}^*}{p_{\mu_2}} \leq \frac{m_{X,0}}{\tau_0} + \frac{\mu_2^+ m_{X,1}}{\tau_1} + \sum_{n=2}^{\infty} \frac{(\mu_2^+)^n m_{X,n}}{\tau_n n!}, \tag{28}$$

$$\frac{e^{\mu_1^+} M_{X,\mu_1}^*}{p_{\mu_1}} \geq \frac{m_{X,0}}{\tau_0} + \frac{\mu_1^- m_{X,1}}{\tau_1} + \sum_{n=2}^{\infty} \frac{(\mu_1^-)^n m_{X,n}}{\tau_n n!}, \tag{29}$$

By adding Equations (28) and (29), we can obtain

$$\frac{(\mu_1^- - \mu_2^+)m_{X,1}}{\tau_1} \leq \frac{e^{\mu_1^+} M^*_{X,\mu_1}}{p_{\mu_1}} - \frac{e^{\mu_1^-} M^*_{X,\mu_2}}{p_{\mu_2}} + \sum_{n=2}^{\infty} \frac{(\mu_2)^n - (\mu_1^-)^n}{\tau_n n!} m_{X,n}. \tag{30}$$

Due to $\mu_1^- \geq \mu_2^2$,

$$m_{X,1} \leq m^U_{X,1} = \frac{\tau_1^+}{\mu_1^- - \mu_2^+} \left(\frac{e^{\mu_1^+} M^{*U}_{X,\mu_1}}{p_{\mu_1}} - \frac{e^{\mu_2^-} M^{*L}_{X,\mu_2}}{p_{\mu_2}} \right). \tag{31}$$

Therefore, we can calculate the upper bound of the phase error rate in the Z basis by Equation (25), and obtain the secret key rate by

$$SKR = \frac{lR_{re}}{N_{total}}, \tag{32}$$

where the R_{re} is the repetition rate of the system and the N_{total} is the number of pulses that Alice needs to send to calculate the amount of the key once.

3. Numerical Simulation

In this section, we simulate a fiber-based QKD system model from [21]. The parameters, namely the intensities μ_i, the relative probability and the probability of choosing the Z basis, are optimized for different channel attenuation.

The system operates at a repetition rate of 1 GHz. For the detectors, we assume that the dead-time t_{dead} is 100 ns and the dark count rate $p_d = 10^{-8}$. In addition, the optical misalignment error rate p_{perr} is fixed to 0.001. The efficiency of error correction f_{EC} is 1.16. The experimental parameters are shown in Table 1.

Table 1. Simulation parameters [21].

Variable	Parameter	Simulation Value
p_d	Dark count rate	10^{-8}
p_{perr}	Optical misalignment error	0.01
t_{dead}	Dead time	100 ns
ε_{sec}	Secrecy parameter	10^{-9}
ε_{cor}	Correctness parameter	10^{-15}
f_{EC}	Efficiency of error correction	1.16

Based on the parameters above, we simulate the secret key rate curve. We firstly simulate the effect of data size on the security key rate, i.e., $N_Z = 10^8, 10^9, 10^{10}, 10^{20}$ for $\delta_\mu = 0, 0.09$. As shown in Figure 1, when the data size is small, the secret key rate is greatly affected by the fluctuation in intensity. The main reason for this impact is that the larger the amount of data, the less sensitive it is to statistical fluctuations. From Equations (5) and (6), we can infer that a large data size can estimate N^*_{α,μ_i} and M^*_{α,μ_i} more closely. Therefore, we can achieve a tighter secure key rate in the later calculation. As the data size increases to a certain extent, its impact on statistical fluctuations will become less obvious and the curves of the secure key rate will converge. In Figure 1 right, the key rate curve decreases rapidly compared with the case without intensity fluctuations when $N_Z = 10^8$ and $\delta_\mu = 0.09$. Intensity fluctuation parameter δ_μ provides us with the range of intensity and helps us to estimate the secure key rate considering the worst case. However, when the data size tends to infinity, the key rate curve is less affected by the intensity fluctuations. Then, we simulate the effects of intensity fluctuations in different degrees on the 1-decoy state method. Assuming the secret key rates with degrees of intensity fluctuations, i.e., $\delta_\mu = 0, 0.01, 0.05, 0.09$, for $N_Z = 10^8$ and $N_Z = 10^9$, respectively. We can see the results in Figure 2. Obviously, the intensity fluctuations have non-negligible effects on the secret key

rate; the transmission distance is significantly reduced with the increase in the intensity fluctuation parameter. As shown in Equations (9), (22), (24) and (25), the counts $s^L_{Z,0}$, $s^L_{Z,1}$ and the phase error ϕ^U_Z are all affected by strength fluctuations, leading to a reduction in the secure key rate. Moreover, the effects of intensity fluctuations are more obvious for $N_Z = 10^8$ than $N_Z = 10^9$.

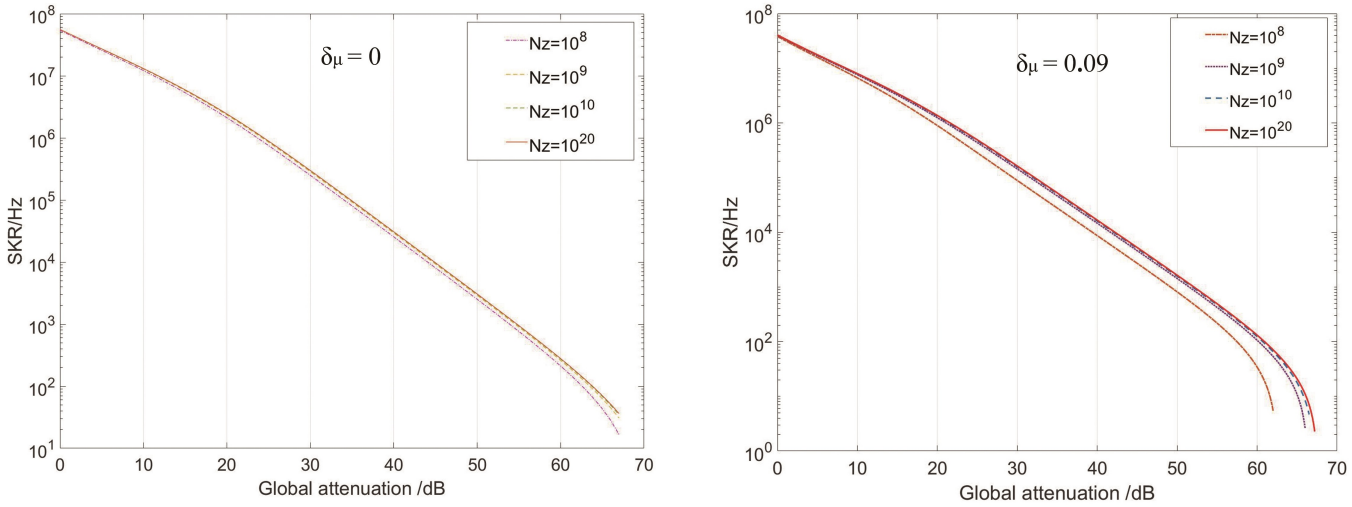

Figure 1. (Color online) Secret key rate vs. global attenuation for $N_Z = 10^8, 10^9, 10^{10}, 10^{20}$ with $\delta_\mu = 0$, 0.09.

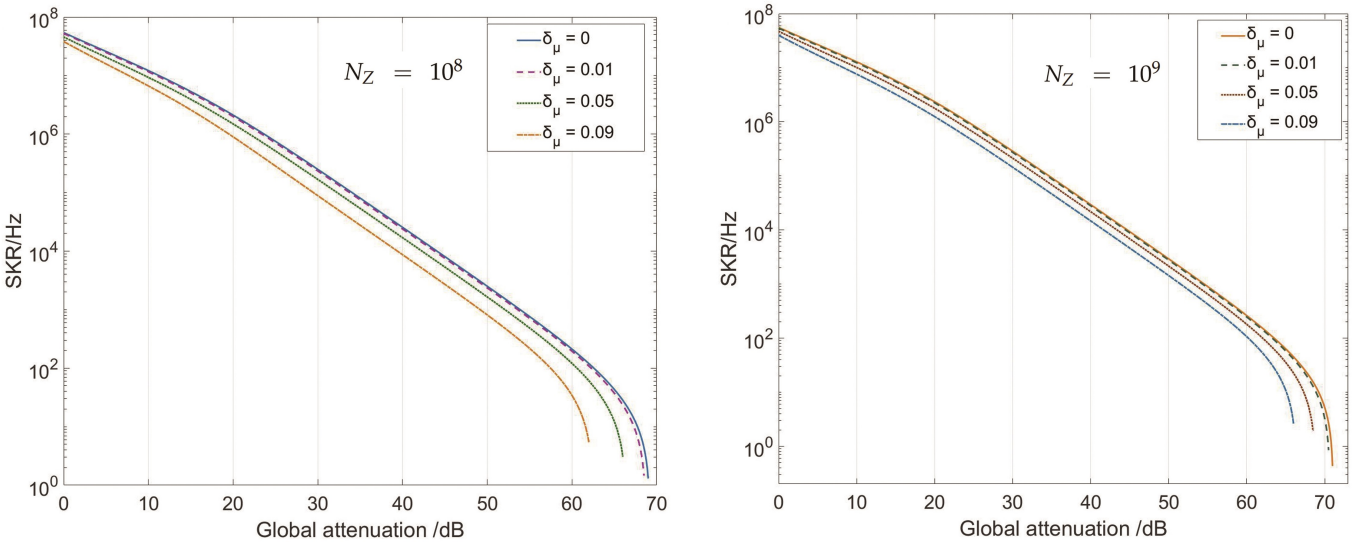

Figure 2. (Color online) Secret key rate vs. global attenuation for $N_Z = 10^8$ and $N_Z = 10^9$ with $\delta_\mu = 0$, 0.01, 0.05, 0.09.

In order to research the effect of δ_μ on the secret key rate for different N_Z, we plot the R_{δ_μ}/R_{ideal} curves. The R_{ideal} means the result without intensity fluctuations and the R_{δ_μ} is the secure key rate under certain intensity fluctuations with the parameter δ_μ. From the discussion above, it is obvious that the intensity fluctuation parameter δ_μ has a negligible impact on the secure key rate. The relations between R_{δ_μ}/R_{ideal} and the global attenuation with δ_μ= 0.01, 0.05, 0.09 for $N_Z = 10^8$ and $N_Z = 10^9$ are shown in Figure 3.

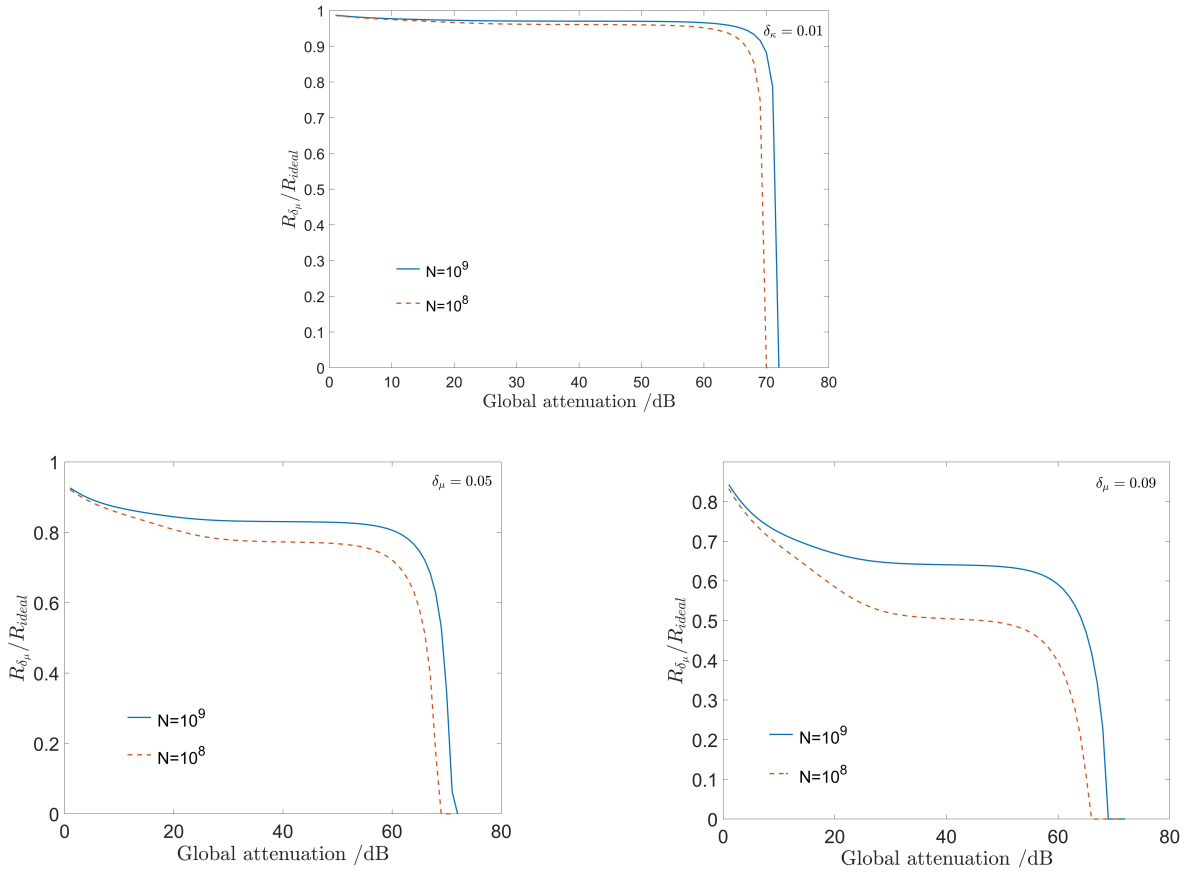

Figure 3. (Color online) R_{δ_μ}/R_{ideal} vs. global attenuation for $N_Z = 10^8$ and $N_Z = 10^9$ with δ_μ = 0, 0.01, 0.05, 0.09.

As can be seen from the figure, the stronger the intensity fluctuations, the more obvious the downward trend of the security key rate. In addition, the key rate is less affected by the intensity fluctuations during normal attenuation. However, when the global attenuation exceeds 60 dB, the security key rate decreases sharply, especially when $N_Z = 10^8$. In this part, we simulate the effect of the intensity fluctuations to the secret key rate of the 1-decoy state method with finite-length data sizes. The simulation results show that the secret key rate of the 1-decoy state method is sensitive to intensity fluctuations.

4. Conclusions

The 1-decoy state protocol has been proven to have better performance in practical applications under normal attenuation. In this paper, we presented a finite-key analysis of the practical 1-decoy method with intensity fluctuations based on Azuma's inequality. We derived the formulas to bound the single-photon events and the phase error rate with both finite-key effects and intensity fluctuations. Our results show that when the data size is relatively small, the single decoy state protocol is greatly affected by the finite-length key and strength fluctuations. The results can also be reflected in the process of deriving the formula for the secure key rate. In the process of implementing practical 1-decoy state QKD, it is necessary to set an appropriate data size before the post-processing to alleviate the influence of statistical fluctuations on the secure key rate. The set data size does not need to be too large, as it takes a long time to collect the data and the advantage of one decoy state over two decoy states will disappear. According to our simulation, the accurate estimation of the intensity fluctuations plays a significant role in the secure analysis, especially for a small data size of the total transmitting signals. For intensity fluctuations, we can measure the range of intensity before the protocol. If the range of intensity fluctuations exceeds a certain threshold, we have to replace the laser. In this paper, we propose a method to

estimate the secure key rate for the 1-decoy state protocol when considering the different intensity fluctuations; otherwise, it will overestimate the secret information and bring the hidden danger of information disclosure. Moreover, when we consider both finite-length keys and intensity fluctuations, the protocol with data size $N = 10^9$ performs better than the protocol with data size $N = 10^8$, especially when the intensity fluctuation parameter $\delta_\mu = 0.09$.

Author Contributions: Conceptualization, C.Z. and Y.Z.; methodology, C.Z., Y.X. and Y.W.; software, Y.Z. and Y.W.; writing—original draft preparation, C.Z., Y.Z. and Y.L.; writing—review and editing, Y.X., M.J. and X.Z.; project administration, W.B.; funding acquisition, W.B. and C.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key Research and Development Program of China (Grant No. 2020YFA0309702), the National Natural Science Foundation of China (Grant Nos. 61505261, 62101597, 61605248 and 61675235), the China Postdoctoral Science Foundation (Grant No. 2021M691536), the Natural Science Foundation of Henan (Grant Nos. 202300410534 and 202300410532) and the Anhui Initiative in Quantum Information Technologies.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **1984**, *560*, 7–11. [CrossRef]
2. Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. Experimental Quantum Cryptography. In Proceedings of the Advances in Cryptology—EUROCRYPT, Brighton, UK, 8–11 April 1991; Springer: Berlin/Heidelberg, Germany, 1991.
3. Yin, H.-L.; Chen, T.-Y.; Yu, Z.-W.; Liu, H.; You, L.-X.; Zhou, Y.-H.; Chen, S.-J.; Mao, Y.; Huang, M.-Q.; Zhang, W.-J.; et al. Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber. *Phys. Rev. Lett.* **2016**, *117*, 190501. [CrossRef] [PubMed]
4. Liao, S.-K.; Liao, S.-K.; Cai, W.-Q.; Liu, W.-Y.; Zhang, L.; Li, Y.; Ren, J.-G.; Yin, J.; Shen, Q.; Cao, Y.; et al. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549*, 43–47. [CrossRef] [PubMed]
5. 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]
6. Makarov, V.; Anisimov, A.; Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **2006**, *74*, 022313. [CrossRef]
7. Lamas-Linares, A.; Kurtsiefer, C. Breaking a quantum key distribution system through a timing side channel. *Opt. Express* **2007**, *15*, 9388–9393. [CrossRef]
8. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **2010**, *4*, 686–689. [CrossRef]
9. Huttner, B.; Imoto, N.; Gisin, N.; Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* **1995**, *51*, 1863. [CrossRef]
10. Brassard, G.; Lütkenhaus, N.; Mor, T.; Sanders, B.C. Security aspects of practical quantum cryptography. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Bruges, Belgium, 14–18 May 2000; Springer: New York, NY, USA, 2000.
11. Brassard, G.; Lütkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **2000**, *85*, 1330. [CrossRef]
12. Hwang, W.-Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef]
13. Lo, H.-K.; Ma, X.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef] [PubMed]
14. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef] [PubMed]
15. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 012326. [CrossRef]
16. Wang, X.-B.; Yang, L.; Peng, C.Z.; Pan, J.W. Decoy-state quantum key distribution with both source errors and statistical fluctuations. *New J. Phys.* **2009**, *11*, 075006. [CrossRef]
17. Wang, S.; Zhang, S.-L.; Li, H.-W.; Yin, Z.-Q.; Zhao, Y.-B.; Chen, W.; Han, Z.-F.; Guo, G.-C. Decoy-state theory for the heralded single-photon source with intensity fluctuations. *Phys. Rev. A* **2009**, *79*, 062309. [CrossRef]

18. Wang, Y.; Bao, W.S.; Zhou, C.; Jiang, M.S.; Li, H.W. Tight finite-key analysis of a practical decoy-state quantum key distribution with unstable sources. *Phys. Rev. A* **2016**, *94*, 032335. [CrossRef]
19. Zhou, C.; Bao, W.; Fu, X. Decoy-state quantum key distribution for the heralded pair coherent state photon source with intensity fluctuations. *Sci. China Inf. Sci.* **2010**, *53*, 2485–2494. [CrossRef]
20. Azuma, K. Weighted sums of certain dependent random variables. *Tohoku Math. J. Second. Ser.* **1967**, *19*, 357–367. [CrossRef]
21. Rusca, D.; Boaron, A.; Grünenfelder, F.; Martin, A.; Zbinden, H. Finite-key analysis for the 1-decoy state QKD protocol. *Appl. Phys. Lett.* **2018**, *112*, 171104. [CrossRef]
22. Hoeffding, W. Probability Inequalities for Sums of Bounded Random Variables. *J. Am. Stat. Assoc.* **1963**, *58*, 13–30. [CrossRef]
23. Chernoff, H. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Ann. Math. Stat.* **1952**, *23*, 493–507. [CrossRef]
24. Zhang, Z.; Zhao, Q.; Razavi, M.; Ma, X. Improved key-rate bounds for practical decoy-state quan-tum-key-distribution systems. *Phys. Rev. A* **2017**, *95*, 012333. [CrossRef]
25. Ma, X.; Fung, C.-H.F.; Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **2012**, *86*, 052305. [CrossRef]
26. He, S.-F.; Wang, Y.; Li, J.J.; Bao, W.S. Asymmetric twin-field quantum key distribution with both statis-tical and intensity fluctuations. *Commun. Theor. Phys.* **2020**, *72*, 065103. [CrossRef]
27. Li, C.; Qian, L.; Lo, H.-K. Simple security proofs for continuous-variable quantum key distribution with intensity fluctuating sources. *arXiv* **2019**, arXiv:190811423.
28. Liu, K.; Li, J.; Zhu, J.R.; Zhang, C.M.; Wang, Q. Decoy-state reference-frame-independent quantum key distribution with both source errors and statistical fluctuations. *Chin. Phys. B* **2017**, *26*, 120302. [CrossRef]
29. Fung, C.-H.F.; Ma, X.; Chau, H. Practical issues in quantum-key-distribution postprocessing. *Phys. Rev. A* **2010**, *81*, 012318. [CrossRef]