entropy

MDPI

Article

Detecting a Photon-Number Splitting Attack in Decoy-State Measurement-Device-Independent Quantum Key Distribution via Statistical Hypothesis Testing

Xiaoming Chen [1,2,3], Lei Chen [1,2,*] and Yalong Yan [3]

[1] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2] Beijing Electronic Science and Technology Institute, Beijing 100070, China
[3] School of Cyber Science and Technology, University of Science and Technology of China, Hefei 230026, China
* Correspondence: chenlei1992@bupt.edu.cn

Abstract: Measurement-device-independent quantum key distribution (MDI-QKD) is innately immune to all detection-side attacks. Due to the limitations of technology, most MDI-QKD protocols use weak coherent photon sources (WCPs), which may suffer from a photon-number splitting (PNS) attack from eavesdroppers. Therefore, the existing MDI-QKD protocols also need the decoy-state method, which can resist PNS attacks very well. However, the existing decoy-state methods do not attend to the existence of PNS attacks, and the secure keys are only generated by single-photon components. In fact, multiphoton pulses can also form secure keys if we can confirm that there is no PNS attack. For simplicity, we only analyze the weaker version of a PNS attack in which a legitimate user's pulse count rate changes significantly after the attack. In this paper, under the null hypothesis of no PNS attack, we first determine whether there is an attack or not by retrieving the missing information of the existing decoy-state MDI-QKD protocols via statistical hypothesis testing, extract a normal distribution statistic, and provide a detection method and the corresponding Type I error probability. If the result is judged to be an attack, we use the existing decoy-state method to estimate the secure key rate. Otherwise, all pulses with the same basis leading to successful Bell state measurement (BSM) events including both single-photon pulses and multiphoton pulses can be used to generate secure keys, and we give the formula of the secure key rate in this case. Finally, based on actual experimental data from other literature, the associated experimental results (e.g., the significance level is 5%) show the correctness of our method.

Keywords: decoy state; measurement-device independent; quantum key distribution; photon number splitting attack; statistical hypothesis testing

Citation: Chen, X.; Chen, L.; Yan, Y. Detecting a Photon-Number Splitting Attack in Decoy-State Measurement-Device-Independent Quantum Key Distribution via Statistical Hypothesis Testing. *Entropy* **2022**, *24*, 1232. https://doi.org/10.3390/e24091232

Academic Editor: Osamu Hirota

Received: 11 July 2022
Accepted: 23 August 2022
Published: 2 September 2022

1. Introduction

Quantum key distribution (QKD) [1–6] is a technique that allows two remote parties (Alice and Bob), to share unconditional secure keys. The unconditional security of the keys are guaranteed by the laws of quantum mechanics [7–10]. The first ideal QKD protocol is BB84-QKD created by Bennett and Brassard [1], which needs a perfect single-photon source and detectors. However, there is always a large gap between ideal and reality. Due to the imperfection of equipment, the implementation of the QKD suffers double attacks from the source side and detection side. On the one hand, at present, perfect single-photon sources are not available, and weak coherent photon sources (WCPs) after phase randomization are often utilized to replace the single-photon sources. While the photon number of the pulses emitted by WCPs may be more than one, an eavesdropper Eve can launch a photon-number splitting (PNS) attack [11–15]. Specially, a weaker version of a PNS attack is one in which Alice's or Bob's pulse count rate changes significantly after the attack [11–14], and the stronger PNS attack means that both Alice's and Bob's pulse count rates remain unchanged after the attack [15]. The difference between these two attacks is the effect on Alice's and

Bob's pulse count rates. Fortunately, the decoy-state method [16–18] proposed later can resist PNS attacks very well.

On the other hand, due to the low detection efficiency of the detectors, Eve can launch attacks against the detectors. Compared with source attacks, there are more attacks from the detection side, such as the detector blinding attack [19,20], dead time attack [21], faked state attack [22,23], and time shift attack [24].People have proposed device-independent quantum key distribution (DI-QKD) [25,26], which can resist all attacks from devices. However, this protocol is highly impractical because it needs close to unity detection efficiency. In 2012, Lo et al. [27] proposed measurement-device-independent quantum key distribution (MDI-QKD), which is also known as the time-inversion version of EPR protocol [28]. In MDI-QKD, Alice and Bob do not need to perform measurement operations, so it can be innately immune to all detection attacks. MDI-QKD combined with the decoy-state method can resist both source attacks and detection attacks; thus, decoy-state MDI-QKD [29–31] is one of the most promising QKD protocols, which can provide unconditional secure keys in practical applications.

However, the secure key rate of the existing decoy-state MDI-QKD is not high [32,33]. The decoy-state method defeats the PNS attack through providing a more accurate method to determine the secure key rate. More specifically, the existing decoy-state method can more closely estimate the lower bound of gain and the upper bound of quantum bit error rate (QBER) of single-photon signals, and then the secure key rate can be calculated by the GLLP formula [34]. In essence, the existing decoy-state method does not care about the existence of a PNS attack, and the secure keys are only generated by single-photon components [35]. However, if we can determine that there is no PNS attack on the channel, multiphoton pulses can also generate secure keys. For simplicity, we only analyze the weaker version of PNS attack in which the legitimate user's pulse count rate changes significantly after the attack. In this case, there is no doubt that using the existing methods to estimate the secure key rate will waste the underlying keys generated from multiphoton pulses and reduce the efficiency.

In this work, under the null hypothesis of no PNS attack H_0, we first retrieve the lost information in the existing decoy-state MDI-QKD, extract a normal distribution statistic, and provide a new method to determine whether there is a PNS attack or not through statistical hypothesis testing. If the result is judged to be an attack, the keys can only be generated from single-photon pulses, and the secure key rate will be estimated by the existing decoy-state method. Otherwise, all pulses with the same basis leading to a successful Bell state measurement (BSM) event including both single-photon pulses and multiphoton pulses can be used to generate keys, and we give the formula of the secure key rate in this case. Furthermore, we use the real experimental data in [36] to verify our method, and the analytical results show that our method is credible (e.g., a significance level of 5%).

The structure of this paper is organized as follows. In Section 2, we briefly review the typical decoy-state MDI-QKD and related notations. In Section 3, we describe our method for detecting the PNS attack in the decoy-state MDI-QKD via statistical hypothesis testing in detail. In Section 4, the correctness of our method is verified with the real experimental data from the existing literature. Finally, we discuss and draw conclusions in Section 5.

2. Three-Intensity Decoy-State MDI-QKD

In this paper, we adopt a typical decoy-state MDI-QKD with polarization encoding [36], which mainly consists of three steps.

(i) Alice generates phase-randomized pulses from WCPs and randomly selects the basis $W \in \{Z, X\}$. That is, $P_Z = P_X = 1/2$, where P_Z and P_X are the probabilities of choosing the Z basis and X basis, respectively. Then Alice uses an intensity modulator to modulate the pulses with three different intensities and sends them to Charlie located in the middle. This three intensities are the intensity of signal state μ_2, the intensity of decoy state μ_1, and the intensity of vacuum state μ_0, respectively. Furthermore, the

corresponding percentages being emitted are P_{μ_2}, P_{μ_1}, and P_{μ_0}, respectively. Obviously, $P_{\mu_2} + P_{\mu_1} + P_{\mu_0} = 1$. At the same time, Bob performs the same procedures as Alice, and the intensities of Bob's pulses are noted as ν_2, ν_1, and ν_0 for the signal state, decoy state, and vacuum state, respectively. Similarly, the corresponding percentages being emitted are P_{ν_2}, P_{ν_1}, and P_{ν_0}, respectively, where $P_{\nu_2} + P_{\nu_1} + P_{\nu_0} = 1$.

(ii) The pulses from Alice and Bob interfere when they reach Charlie. Then Charlie performs a Bell state measurement (BSM) on the interference outcomes and announces the measurement results to Alice and Bob.

(iii) Alice and Bob compare their bases, and determine the secure keys through Charlie's measurement results. Specifically, if Alice and Bob choose the same basis and Charlie has a successful BSM event at the same time, then this part of the pulses can generate keys. It is important to emphasize that the secure keys are only generated from the signal state with Z basis, and the others are used for parameter estimation.

The secure key rate of the decoy-state MDI-QKD [27,36] is given by

$$R \geq q\{P_{11}^{\mu_2\nu_2} Y_{11}^{Z}[1 - H(e_{11}^{X})] - Q_{\mu_2\nu_2}^{Z} f_e H(E_{\mu_2\nu_2}^{Z})\}. \tag{1}$$

In the above equation, $q = P_Z^2 P_{\mu_2} P_{\nu_2}$ is the probability that Alice and Bob both select the Z basis and both modulate the pulse as signal state. $P_{11}^{\mu_2\nu_2} = \mu_2\nu_2 e^{-\mu_2-\nu_2}$ is the probability that the pulses from Alice's signal state and Bob's signal state are both single-photon pulses. Y_{11}^{Z} and e_{11}^{X} are the yield of single-photon state with Z basis and the quantum bit error rate (QBER) of single-photon state with X basis. $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. $Q_{\mu_2\nu_2}^{Z}$ and $E_{\mu_2\nu_2}^{Z}$ are the overall gain and overall QBER of signal state with Z basis, respectively. $f_e > 1$ is the error correction efficiency.

According to [37,38], the overall gain $Q_{\mu_k\nu_l}^{W}$ $(W \in \{X, Z\})$ and the overall QBER $E_{\mu_k\nu_l}^{W}$ $(W \in \{X, Z\})$ can be obtained by the following equations,

$$\begin{aligned} Q_{\mu_k\nu_l}^{X} &= 2y^2[1 + 2y^2 - 4yI_0(x) + I_0(2x)], \\ E_{\mu_k\nu_l}^{X} Q_{\mu_k\nu_l}^{X} &= e_0 Q_{\mu_k\nu_l}^{X} - 2(e_0 - e_d)y^2[I_0(2x) - 1], \\ Q_{\mu_k\nu_l}^{Z} &= Q_C + Q_E, \\ E_{\mu_k\nu_l}^{Z} Q_{\mu_k\nu_l}^{Z} &= e_d Q_C + (1 - e_d) Q_E. \end{aligned} \tag{2}$$

where

$$\begin{aligned} Q_C &= 2(1-p_d)^2 e^{-\mu'/2}[1 - (1-p_d)e^{-\eta_a\mu_k/2}] \times [1 - (1-p_d)e^{-\eta_b\nu_l/2}], \\ Q_E &= 2p_d(1-p_d)^2 e^{-\mu'/2}[I_0(2x) - (1-p_d)e^{-\mu'/2}]. \end{aligned} \tag{3}$$

In the above equations, μ_k and ν_l, $k, l \in \{0, 1, 2\}$, are the intensities of pulses emitted by Alice and Bob, respectively. $I_0(x)$ is the modified Bessel function of the first kind. e_0 is the error rate of background. e_d is the misalignment-error probability. p_d is the dark count rate. η_a and η_b are the transmission efficiencies of Alice and Bob, respectively. In addition,

$$\begin{aligned} x &= \sqrt{\eta_a\mu_k\eta_b\nu_l}/2, \\ y &= (1-p_d)e^{-\mu'/4}, \\ \mu' &= \eta_a\mu_k + \eta_b\nu_l, \\ \eta_a &= \eta_d 10^{-\frac{\delta L_{ac}+\theta}{10}}, \\ \eta_b &= \eta_d 10^{-\frac{\delta L_{bc}+\theta}{10}}, \end{aligned} \tag{4}$$

where η_d is the quantum efficiency of detectors, δ is the loss coefficient measured in dB/km, L_{ac} (L_{bc}) is the distance in km from Alice (Bob) to Charlie, and θ is the insertion loss in Charlie's measurement setup in dB. Without Eve's intervention, based on Equations (2)–(4),

the yield and the QBER of single-photon pulses when Alice and Bob select the same basis X or Z are, respectively, given by

$$\begin{aligned} Y_{11}^X = Y_{11}^Z &= (1-p_d)^2[\frac{\eta_a\eta_b}{2} + (2\eta_a + 2\eta_b - 3\eta_a\eta_b)p_d + 4(1-\eta_a)(1-\eta_b)p_d^2], \\ e_{11}^X Y_{11}^X &= e_0 Y_{11}^X - (e_0 - e_d)(1-p_d)^2\frac{\eta_a\eta_b}{2}, \\ e_{11}^Z Y_{11}^Z &= e_0 Y_{11}^Z - (e_0 - e_d)(1-p_d)^2(1-p_d)\frac{\eta_a\eta_b}{2}. \end{aligned} \tag{5}$$

3. Statistical Hypothesis Testing

In this section, we introduce a new method to detect the PNS attack in the decoy-state MDI-QKD via statistical hypothesis testing. It is important to emphasize that the PNS attacks mentioned here and below refer to the weaker version of PNS attack. Then we analyze the Type I error of the test; that is, mistaking no PNS attack when there is a PNS attack. Generally speaking, our method first puts forward a null hypothesis and alternative hypothesis based on the theory of statistical hypothesis testing. Then, the test statistic is constructed according to the null hypothesis and other conditions. Furthermore, the specific values of the statistics can be obtained by using the parameters and experimental data. After the significance level is given, we can infer whether there is PNS attack in the channel with a certain probability. The details are as follows.

(i) Identify null and alternative hypothesis. Let us consider the hypothesis testing problem of the null hypothesis H_0: there is no PNS attack on the channel and the alternative hypothesis H_1: there is a PNS attack on the channel.

(ii) Construct the test statistic. We need a test statistic to conduct the hypothesis testing. In what follows, the distribution of the test statistic is derived under the null hypothesis H_0. Let us further consider Alice's and Bob's pulses emission process and Charlie's BSM event. When Alice and Bob send pulses with the same basis, the BSM event outcomes at Charlie only include two cases, successful or failed. Therefore, the above process can be regarded as a Bernoulli trial. Note that $Q_{\mu_k\nu_l}^W$ is the probability that Charlie obtains a successful BSM event provided that Alice and Bob emit pulses with the intensities μ_k and ν_l and select the basis W. Suppose the total number of pulses emitted by Alice (Bob) is N_{data}, then the number of pulses is $P_W^2 P_{\mu_k\nu_l} N_{data}$ when Alice's and Bob's intensities with W basis are μ_k and ν_l, respectively. In the above equation, P_W is the probability that Alice (Bob) chooses the $W \in \{X, Z\}$ basis, $P_{\mu_k\nu_l} = P_{\mu_k} P_{\nu_l}$ is the probability that Alice and Bob choose the intensities μ_k and ν_l, respectively. At this point, the number of successful BSM events that Charlie obtained is denoted as $n_{\mu_k\nu_l}^W$. Then, $n_{\mu_k\nu_l}^W$ has the binomial distribution with parameters $(P_W^2 P_{\mu_k\nu_l} N_{data},\ Q_{\mu_k\nu_l}^W)$, for short,

$$n_{\mu_k\nu_l}^W \sim B(P_W^2 P_{\mu_k\nu_l} N_{data},\ Q_{\mu_k\nu_l}^W). \tag{6}$$

According to [36], we find N_{data} is so large (typically $10^{10} \sim 10^{11}$), $Q_{\mu_k\nu_l}^W$ is close to $10^{-8} \sim 10^{-5}$. Generally, the selections of basis and intensity are random. In other words, $P_Z = P_X = 1/2$, $P_{\mu_k} = P_{\nu_l} = 1/3$ where $k, l \in \{0, 1, 2\}$. Thus, we have $P_W^2 P_{\mu_k\nu_l} N_{data} Q_{\mu_k\nu_l}^W > P_W^2 P_{\mu_k\nu_l} N_{data}(1 - Q_{\mu_k\nu_l}^W) \geq 5$. By the law of large numbers and the central limit theorem, when $P_W^2 P_{\mu_k\nu_l} N_{data} Q_{\mu_k\nu_l}^W \geq 5$ and $P_W^2 P_{\mu_k\nu_l} N_{data}(1 - Q_{\mu_k\nu_l}^W) \geq 5$, the binomial distribution with parameters $(P_W^2 P_{\mu_k\nu_l} N_{data},\ Q_{\mu_k\nu_l}^W)$ can be approximately regarded as the normal distribution with mean $P_W^2 P_{\mu_k\nu_l} N_{data} Q_{\mu_k\nu_l}^W$ and variance $P_W^2 P_{\mu_k\nu_l} N_{data}(1 - Q_{\mu_k\nu_l}^W)$, given by

$$n_{\mu_k\nu_l}^W \sim N(P_W^2 P_{\mu_k\nu_l} N_{data} Q_{\mu_k\nu_l}^W,\ P_W^2 P_{\mu_k\nu_l} N_{data}(1 - Q_{\mu_k\nu_l}^W)). \tag{7}$$

After standardization, we obtain a random variable $U^W_{\mu_k\nu_l}$, which obeys the standard normal distribution; that is,

$$U^W_{\mu_k\nu_l} = \frac{n^W_{\mu_k\nu_l} - P^2_W P_{\mu_k\nu_l} N_{data} Q^W_{\mu_k\nu_l}}{\sqrt{P^2_W P_{\mu_k\nu_l} N_{data}(1 - Q^W_{\mu_k\nu_l})}} \sim N(0,1). \tag{8}$$

Considering the additivity of normal distribution, we obtain a random variable involving all possibilities of $U^W_{\mu_k\nu_l}$ where $W \in \{X, Z\}$, $k, l \in \{0, 1, 2\}$, which also obeys the normal distribution. There are eighteen cases of $U^W_{\mu_k\nu_l}$ considering that the pair of intensity is nine cases and the selection of basis is two cases. Note that we only consider the same basis for Alice and Bob, that is, both Z basis or both X basis. After standardization, we obtain a new random variable V that obeys the standard normal distribution, which can be written as

$$V = \frac{1}{\sqrt{18}} \sum_{W\in\{Z,X\},\, k,\, l\in\{0,1,2\}} \frac{n^W_{\mu_k\nu_l} - P^2_W P_{\mu_k\nu_l} N_{data} Q^W_{\mu_k\nu_l}}{\sqrt{P^2_W P_{\mu_k\nu_l} N_{data}(1 - Q^W_{\mu_k\nu_l})}} \sim N(0,1). \tag{9}$$

Furthermore, $\Phi(v)$ is the distribution function of V, given by

$$\Phi(v) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{v} e^{-\frac{t^2}{2}} \mathrm{d}t, \ -\infty < vs. < \infty, \tag{10}$$

where v is the value of V and is just the test statistic that we find.

(iii) Find the value of the test statistic. We set the parameters N_{data}, e_d, e_0, p_d, L_{ac}, L_{bc}, δ, θ, P_Z, P_X, μ_k, ν_l, P_{μ_k}, and P_{ν_l}, where $k, l \in \{0, 1, 2\}$, and we calculate the theoretical value of $Q^W_{\mu_k\nu_l}$ according to Equations (2)–(4). We record $n^W_{\mu_k\nu_l}$ where $k, l \in \{0, 1, 2\}$, $W \in \{X, Z\}$. We substitute the above data into Equation (9) and obtain the value of the test statistic v.

(iv) Choose a significance level. We need to determine a significance level α (typically 0.05) for the test. In terms of the null hypothesis H_0 of the test, we deduce that the test is a two-tailed hypothesis testing. Given α, the rejection region is $|vs.| > v_{[1-\alpha/2]}$ where $v_{[1-\alpha/2]}$ can be obtained by Equation (10). More precisely, the variables $-v_{[1-\alpha/2]}$ and $v_{[1-\alpha/2]}$ refer to the boundary values between the rejection region and the acceptance region for the test. Let the left side of Equation (10) be equal to $\alpha/2$; the upper limit of the integral will be $-v_{[1-\alpha/2]}$. According to the symmetry of the probability density function of normal distribution, $v_{[1-\alpha/2]}$ can be obtained.

(v) Make a decision. Compare the test statistic v with the critical values $v_{[1-\alpha/2]}$ and $-v_{[1-\alpha/2]}$. If $v > v_{[1-\alpha/2]}$ or $v < -v_{[1-\alpha/2]}$, we will reject H_0 and accept H_1. This means that we believe there is a PNS attack on the channel. Otherwise, we fail to reject H_0. That is to say, we consider there is no PNS attack on the channel. Note that the significance level of the test α is just the Type I error probability of the test, namely, the probability of mistaking no PNS attack for having a PNS attack. Let β denote the Type II error probability of the test, to be precise, the probability of mistaking having a PNS attack for no PNS attack. Note that β is usually difficult to solve in most situations. Furthermore, determining the value of β requires more information about the aggression behavior.

If the result is judged to be a PNS attack, the secure key rate in this case can be estimated by Equation (1). Otherwise, all pulses with the Z basis leading to a successful BSM event including both single-photon pulses and multiphoton pulses can be used to generate the keys. Furthermore, the secure key rate formula Equation (1) becomes

$$R \geq qQ^Z_{\mu_2\nu_2}[1 - f_e H(E^Z_{\mu_2\nu_2}) - H(E^Z_{\mu_2\nu_2})]. \tag{11}$$

By comparing Equation (11) with Equation (1), we can easily find the secure key rate has been highly improved when the judgment result is no PNS attack. This is mainly due to the contribution of multiphoton components.

4. Results and Analysis

In the preceding section, we showed the details of our detection method. Now, we move forward to the corresponding experiments based on the aforementioned method and analyze the experimental results. Generally speaking, the real experimental data were substituted into the formulas in Section 3 to verify the correctness of our method. The experimental parameters were from real experiments [36]. Specially, the experimenters in [36] adopted a symmetric scheme; that is, all parameters of Alice and Bob were identical and optimized. The relevant experimental parameters used in [36] and this paper are shown in Table 1.

Table 1. Experimental parameters used in this paper. Data from *Phys. Rev. Lett.* **2014**, *112*, 190503.

$\mu_2(\nu_2)$	$\mu_1(\nu_1)$	$\mu_0(\nu_0)$	$P_{\mu_2}(P_{\nu_2})$	$P_{\mu_1}(P_{\nu_1})$	$P_{\mu_0}(P_{\nu_0})$	$P_Z(P_X)$
0.3	0.1	0.01	0.2	0.45	0.35	0.5
N_{data}	e_d	e_0	p_d	$L_{ac}(L_{bc})$	δ	θ
1.69×10^{11}	0.01	0.5	5×10^{-5}	5	0.2	0.8

Based on the above parameters, we can obtain the values of $Q^W_{\mu_k\nu_l}$, as shown in Table 2. Note that Table 2 in this paper is exactly the same as Table I in the Supplementary Materials of [36]. We record the values of $n^W_{\mu_k\nu_l}$, as shown in Table 3. Note that the data in Table 3 can be deduced from Table I in the Main Text of [36]. According to the above data and Equation (8), all values of $U^W_{\mu_k\nu_l}$ can be obtained, as shown in Table 4.

Table 2. The values of $Q^W_{\mu_k\nu_l}(\times 10^{-4})$ with intensities $\mu_k \in \{\mu_2, \mu_1, \mu_0\}$ and $\nu_l \in \{\nu_2, \nu_1, \nu_0\}$ based on $W \in \{X, Z\}$. Reprinted/adapted with permission from Ref. [36], 2014, American Physical Society.

	Z			X		
ν_l \ μ_k	μ_2	μ_1	μ_0	μ_2	μ_1	μ_0
ν_2	0.4643	0.1596	0.0215	0.9086	0.4074	0.2449
ν_1	0.1596	0.0539	0.0066	0.4074	0.1039	0.0319
ν_0	0.0215	0.0066	0.0007	0.2449	0.0319	0.0012

Table 3. The values of $n^W_{\mu_k\nu_l}(\times 10^4)$ with intensities $\mu_k \in \{\mu_2, \mu_1, \mu_0\}$ and $\nu_l \in \{\nu_2, \nu_1, \nu_0\}$ based on $W \in \{X, Z\}$.

	Z			X		
ν_l \ μ_k	μ_2	μ_1	μ_0	μ_2	μ_1	μ_0
ν_2	787.5	270.4	38.03	1526	692.9	429.3
ν_1	262.0	89.74	11.83	670.9	172.4	52.73
ν_0	36.17	11.32	1.521	415.7	53.57	2.366

Table 4. The values of $U^W_{\mu_k\nu_l}$ with intensities $\mu_k \in \{\mu_2, \mu_1, \mu_0\}$ and $\nu_l \in \{\nu_2, \nu_1, \nu_0\}$ based on $W \in \{X, Z\}$.

	Z			X		
ν_l \ μ_k	μ_2	μ_1	μ_0	μ_2	μ_1	μ_0
ν_2	1.026	0.6174	3.709	2.415	2.512	10.00
ν_1	−7.100	−3.187	4.016	−10.05	−5.452	−3.197
ν_0	−0.3709	1.004	5.438	1.209	−0.9135	4.154

The schematic diagram of statistical hypothesis testing is illustrated in Figure 1. After calculation, we obtained the value of the test statistic $v = 0.236$. Given the significance

level of the test $\alpha = 0.05$, the critical values were $v_{[1-\alpha/2]} = 1.96$ and $-v_{[1-\alpha/2]} = -1.96$. Since $-1.96 < 0.236 < 1.96$, the test statistic did not fall inside the rejection region, and we failed to reject H_0. In other words, we inferred that there was no PNS attack on the channel, and the corresponding Type I error probability was less than 5%. According to [36], there was indeed no PNS attack in the experiment, which verifies the correctness of our method. Thus, both single-photon and multiphoton components can be used to generate keys in this case. At this time, the secure key rate can be estimated through Equation (11).

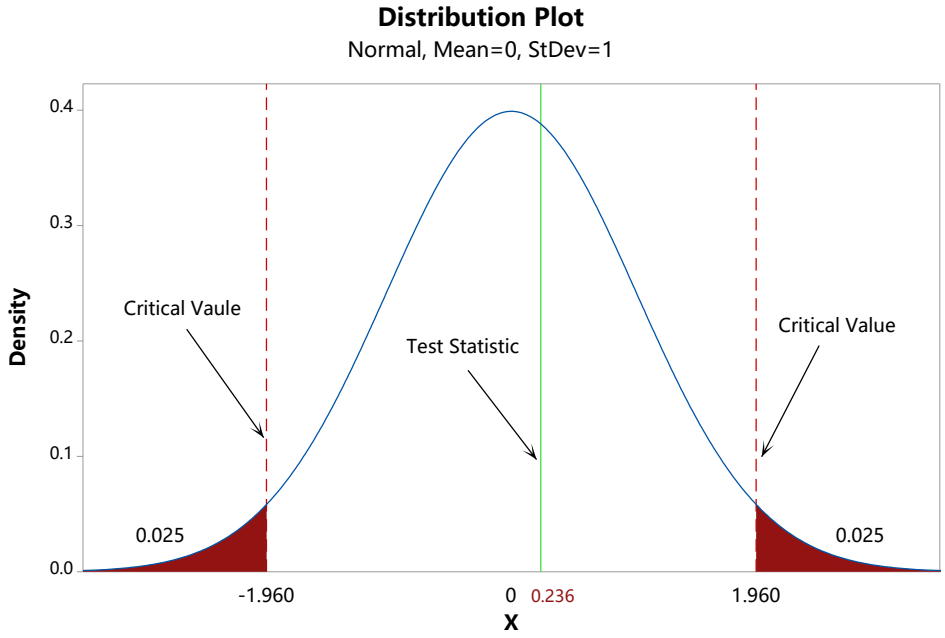

Figure 1. The schematic diagram of statistical hypothesis testing. The value of the test statistic v is 0.236. Given the significance level of the test $\alpha = 0.05$, the critical values are $v_{[1-\alpha/2]} = 1.96$ and $-v_{[1-\alpha/2]} = -1.96$.

5. Conclusions and Discussion

In summary, we first recovered the lost information of the existing decoy-state method when detecting the weaker version of a PNS attack in the decoy-state MDI-QKD and extracted a normal distribution statistic via statistical hypothesis testing. Based on this information, we proposed a new method to detect the weaker version of a PNS attack. Most importantly, the error probability of detection was precisely calculated by our method, and we also gave the calculation. Finally, according to the judgment result, the corresponding secure key rate was provided. In particular, compared with the existing decoy-state MDI-QKD protocols, the secure key rate with our method has been highly improved if the judgment result is no weak PNS attack. Meanwhile, the associated experimental results also verified the correctness of our method.

Nevertheless, all judgment results in this paper were obtained under the condition that the null hypothesis was no weak version of a PNS attack. In other words, we assume that the gain of signal or decoy state will change significantly after the PNS attack. However, we can do nothing about the stronger PNS attack, which retains the gain of signal and decoy state, such as a partial PNS attack [15], because the premise of the derivation no longer holds, and the Type II error probability of our method in this case will be poor even close to unity. For this reason, compared with the existing decoy-state method [29–31] to directly estimate the secure key rate, our method is not ready for practical application now; however, we provide a new direction to improve the secure key rate and efficiency.

Author Contributions: Conceptualization, X.C.; Formal analysis, L.C.; Methodology, L.C.; Writing—original draft, L.C.; Writing—review & editing, Y.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available within the article.

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.* **2014**, *560*, 7. [CrossRef]
2. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441. [CrossRef] [PubMed]
3. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
4. Kraus, B.; Gisin, N.; Renner, R. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.* **2005**, *95*, 080501. [CrossRef]
5. Gisin, N.; Thew, R. Quantum communication. *Nat. Photon.* **2007**, *1*, 165. [CrossRef]
6. Duěk, M.; Lütkenhaus, N.; Hendrych, M. Quantum cryptography. *Prog. Opt.* **2006**, *49*, 381.
7. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802. [CrossRef]
8. Lo, H.K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, *283*, 2050. [CrossRef]
9. Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **2001**, *48*, 351. [CrossRef]
10. Renner, R. Security of quantum key distribution. *Int. J. Quantum Inf.* **2008**, *6*, 1. [CrossRef]
11. Huttner, B.; Imoto, N.; Gisin, N.; Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* **1995**, *51*, 1863. [CrossRef] [PubMed]
12. Brassard, G.; Lütkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **2000**, *85*, 1330. [CrossRef] [PubMed]
13. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **2000**, *61*, 052304. [CrossRef]
14. Liu, W.T.; Sun, S.H.; Liang, L.M.; Yuan, J.M. Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution. *Phys. Rev. A* **2011**, *83*, 042326. [CrossRef]
15. Liu, D.; Wang, S.; Yin, Z.Q.; Chen, W.; Han, Z.F. The security of decoy state protocol in the partial photon number splitting attack. *Chin. Sci. Bull.* **2013**, *58*, 3859. [CrossRef]
16. Hwang, W.Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef] [PubMed]
17. Wang, X.B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef]
18. Lo, H.K.; Ma, X.F.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]
19. Gerhardt, I.; Liu, Q.; Lamas-Linares, A.; Skaar, J.; Kurtsiefer, C.; Makarov, V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2011**, *2*, 349. [CrossRef]
20. Gerhardt, I.; Liu, Q.; Lamas-Linares, A.; Skaar, J.; Scarani, V.; Makarov, V.; Kurtsiefer, C. Experimentally Faking the Violation of Bell's Inequalities. *Phys. Rev. Lett.* **2011**, *107*, 170404. [CrossRef]
21. Henning, W.; Harald, K.; Markus, R.; Martin, F.; Sebastian, N.; Harald, W. Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors. *New J. Phys.* **2004**, *13*, 073024.
22. Makarov, V.; Hjelme, D.R. Faked states attack on quantum cryptosystems. *J. Mod. Opt.* **2005**, *52*, 5. [CrossRef]
23. Makarov, V.; Anisimov, A.; Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **2006**, *74*, 022313. [CrossRef]
24. Qi, B.; Fung, C.H.F.; Lo, H.K.; Ma, X.F. Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.* **2007**, *7*, 73. [CrossRef]
25. Antonio, A.; Nicolas, B.; Nicolas, G.; Serge, M.; Stefano, P.; Valerio, S. Device-Independent Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.* **2007**, *98*, 230501.
26. Stefano, P.; Antonio, A.; Nicolas, B.; Nicolas, G.; Serge, M.; Valerio, S. Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **2009**, *11*, 045021.
27. Lo, H.K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
28. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 6. [CrossRef]

29. Liang, W.T.; Xue, Q.Y.; Jiao, R.Z. The performance of three-intensity decoy-state measurement-device-independent quantum key distribution. *Quantum Inf. Process.* **2020**, *19*, 165. [CrossRef]
30. Lu, F.Y.; Yin, Z.Q.; Fan-Yuan, G.J.; Wang, R.; Liu, H.; Wang, S.; Chen, W.; He, D.Y.; Huang, W.; Xu, B.J.; et al. Efficient decoy states for the reference-frame-independent measurement-device-independent quantum key distribution. *Phys. Rev. A* **2020**, *101*, 052318. [CrossRef]
31. Jiang, C.; Zhou, F.; Wang, X.B. Four-intensity measurement-device-independent quantum key distribution protocol with modified coherent state sources. *Opt. Express* **2022**, *30*, 7. [CrossRef] [PubMed]
32. Tang, Y.L.; Yin, H.L.; Chen, S.J.; Liu, Y.; Zhang, W.J.; Jiang, X.; Zhang, L.; Wang, J.; You, L.X.; Guan, J.Y.; et al. Measurement-Device-Independent Quantum Key Distribution over 200 km. *Phys. Rev. Lett.* **2014**, *113*, 190501. [CrossRef] [PubMed]
33. 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]
34. Gottesman, D.; Lo, H.K.; Lütkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **2004**, *4*, 325.
35. Ma, X.F.; Fung, C.H.F.; Dupuis, F.; Chen, K.; Tamaki, K.; Lo, H.K. Decoy-state quantum key distribution with two-way classical postprocessing. *Phys. Rev. A* **2006**, *74*, 032330. [CrossRef]
36. Tang, Z.T.; Liao, Z.F.; Xu, F.H.; Qi, B.; Qian, L.; Lo, H.K. Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2014**, *112*, 190503. [CrossRef]
37. Ma, X.F.; Fung, C.H.F.; Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **2012**, *86*, 052305. [CrossRef]
38. Ma, X.F.; Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **2012**, *86*, 062319. [CrossRef]