Detecting the possibility of a type of photon number splitting attack in decoy-state quantum key distribution

Xiao-Ming Chen(陈小明)[1,2,3], Lei Chen(陈雷)[1,2,†], and Ya-Long Yan(阎亚龙)[3]

[1] *Beijing University of Posts and Telecommunications, Beijing* 100876, *China*
[2] *Beijing Electronic Science and Technology Institute, Beijing* 100070, *China*
[3] *University of Science and Technology of China, Hefei* 230026, *China*

(Received 9 May 2022; revised manuscript received 5 September 2022; accepted manuscript online 18 October 2022)

The existing decoy-state quantum key distribution (QKD) beating photon-number-splitting (PNS) attack provides a more accurate method to estimate the secure key rate, while it still considers that only single-photon pulses can generate secure keys in any case. However, multiphoton pulses can also generate secure keys if we can detect the possibility of PNS attack in the channel. The ultimate goal of this line of research is to confirm the absence of all types of PNS attacks. In particular, the PNS attack mentioned and detected in this paper is only the weaker version of PNS attack which significantly changes the observed values of the legitimate users. In this paper, under the null hypothesis of no weaker version of PNS attack, we first determine whether there is an attack or not by retrieving the missing information of the existing decoy-state protocols, extract a Cauchy distribution statistic, and further provide a detection method and the type I error probability. If the result is judged to be an attack, we can use the existing decoy-state method and the GLLP formula to estimate the secure key rate. Otherwise, the pulses with the same basis received including both single-photon pulses and multiphoton pulses, can be used to generate the keys and we give the secure key rate in this case. Finally, the associated experiments we performed (i.e., the significance level is 5%) show the correctness of our method.

Keywords: quantum key distribution, photon number splitting, decoy state, hypothesis testing

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/ac9b05

1. Introduction

Quantum key distribution (QKD)[1–7] is a technique that allows two different remote parties, Alice (the sender) and Bob (the receiver), to share a unconditional secret key. The unconditional security of the key is guaranteed through the laws of quantum mechanics.[8–12] The first ideal QKD protocol was BB84-QKD protocol created by Bennett and Brassard,[1] which needs to employ the perfect single-photon source. Nevertheless, at present, single-photon sources are not available, and a weak coherent photon source is often utilized to replace the single-photon source. Due to adopting the imperfect single-photon sources, an eavesdropper Eve can launch the photon-number-splitting (PNS) attack.[13–30] In the basic PNS attack, Eve intercepts the pulse sent by Alice and detects the photon number of the intercepted pulse. If it is a single-photon pulse, it will be directly discarded. If it is a multiphoton pulse, one photon will be stored and the rest will be sent to Bob through a weakly attenuated or even lossless channel. Finally, Eve can obtain exactly the same key as Bob by measuring the stored photons according to the basis published by Alice and Bob, which makes the QKD system no longer secure. Specially, a weaker version of PNS attack is one in which the observed values of Alice and Bob change significantly after the attack,[13–15,29] and the stronger PNS attack means that the observed values of Alice and Bob remain unchanged after the attack.[30] The difference between these two types of attacks is the effect on the observed values of Alice and Bob.

There are numerous protocols proposed to resist the PNS attack, among which the decoy-state method is a highly effective one. In decoy-state QKD, Alice randomly sends pulses from signal source or decoy source, and the only difference between signal source and decoy source is intensity. Importantly, the decoy-state method assumes that Eve could not distinguish the intercepted pulses coming from which source. The existing decoy-state protocols, such as Refs. [31–33], presented a method to defeat the PNS attack. Actually, the decoy-state QKD beats the PNS attack to provide a more accurate method to determine the secure key rate. To be precise, 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 the single-photon signals, and then calculate the secure key rate by using the Gottesman–Lo–Lütkenhaus–Preskill (GLLP) formula[34] inspired by the idea of the entanglement distillation approach,

$$R \geq q\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1 - H_2(e_1)]\}, \tag{1}$$

where q is the basis alignment efficiency depending on the implementation (1/2 for the BB84 protocol), Q_μ and E_μ are, respectively, the gain and QBER of the signal state, $f(E_\mu)$ is the error correction efficiency, $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function, Q_1 and

†Corresponding author. E-mail: chenlei1992@bupt.edu.cn

© 2022 Chinese Physical Society and IOP Publishing Ltd

e_1 are, respectively, the gain and QBER of single-photon states. Unfortunately, the secure key rate of decoy-state QKD is not high, and most of previous literatures use optimization and joint constraints to improve the key rate.[35–38] We find that the existing decoy-state method still considers that only single-photon pulses can generate secure keys in any case. However, if we can detect the possibility of PNS attack in the channel, multiphoton pulses can also generate secure keys. In this case, there is no doubt that using the above method to estimate secure key rate will waste the keys generated by multiphoton pulses and reduce the efficiency. It should be noted that the ultimate goal of this line of research is to confirm the absence of all types of PNS attacks. In particular, the PNS attack mentioned and detected in this paper is only a weaker version of PNS attack which significantly changes the observed values of Alice and Bob.

In this work, under the null hypothesis of no weaker version of PNS attack H_{o1}, we first retrieve the lost information, extract a Cauchy distribution statistic and provide a new method to detect the possibility of PNS attack which significantly changes the observed values of legitimate users in the channel, namely, the first test in this paper. Furthermore, given the significance level of the first test α_1 and the number of the first test m, we interpret the empirical results to verify the correctness of the first test through the NIST Statistical Test Suite,[39] which is called the second test in this paper. If the result is judged to be an attack, the lower bound of the gain and the upper bound of QBER of the single-photon signals will be estimated by the existing decoy-state method, and then the secure key rate will be calculated by the GLLP formula. Otherwise, the pulses with the same basis received including both single-photon pulses and multiphoton pulses, can be used to generate the keys and we also give the secure key rate in this case. And the end, the associated experiments we performed also indicate that our method is credible (i.e., the significance level is 5%).

2. The scheme

In this section, we will focus on our scheme to detect the type of PNS attack which significantly changes the observed values of Alice and Bob. Unless otherwise specified, the PNS attacks mentioned in this paper are both the weaker version. For one thing, we describe the first test, a new detection method of weaker PNS attack for decoy-state QKD, which can precisely calculate the error probability of detection. For another, we interpret the empirical results to verify the correctness of the first test, namely, the second test in this paper. We refer specifically to the interpretation of empirical results in section 4.2 of Ref. [39], which is called the second test in our paper. Two scenarios typify events that may occur due to empirical testing. Case 1: The significance level selected for the first test is reasonable, indicating that the first test is correct. Case 2: The significance level selected for the first test is unreasonable, indicating that the first test is wrong. We use the second test to check the correctness of the first test. Finally, according to the judgment result, we will give the corresponding secure key rate.

2.1. The first test

In this part, we introduce the new method to detect the PNS attack which significantly changes the observed values of legitimate users in decoy-state QKD via statistical hypothesis testing, which is called the first test in this paper. Then we analyze the type I error of the first test, that is, mistaking no PNS attack for having a PNS attack. The first test contains five steps.

Identify null and alternative hypothesis Let us consider the hypothesis testing problem about the null hypothesis H_{o1}: there is no weaker version of PNS attack on the channel and the alternative hypothesis H_{a1}: there is a weaker version of PNS attack on the channel.

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_{o1}. Alice intentionally and randomly selects two weak coherent photon sources with different intensities, after phase randomization, namely, signal source and decoy source. Suppose the intensities of the signal source and the decoy source are μ and ν, respectively. $P_n(\mu)$ denotes the probability of emitting n-photons pulses from the signal source, written as

$$P_n(\mu) = \frac{\mathrm{e}^{-\mu}(\mu)^n}{n!}. \tag{2}$$

The yield y_n represents the probability of receiving a pulse (at Bob's side) after Alice emits a n-photons pulse. According to Ref. [33], one has $y_n \approx n\eta$ where η is the overall transmission probability of each photon. The gain Q is the probability of receiving a pulse (at Bob's side) after Alice emits a pulse, no matter how many photons which contains. The gain of the signal source Q_μ is given by

$$Q_\mu = \sum_{n=0}^{\infty} P_n(\mu) y_n \approx \sum_{n=0}^{\infty} P_n(\mu) n\eta = \eta \sum_{n=0}^{\infty} P_n(\mu) n = \mu\eta. \tag{3}$$

Let us consider further about the sending and receiving process between Alice and Bob. When Alice emits a pulse from the signal source, the outcome (at Bob's side) only includes two cases, that is, receiving it or not. Therefore, the sending and receiving process can be regarded as a Bernoulli trial. Taking the advantage of Eq. (3), we derive the probability that Bob receives the signal pulse $p_1 = \mu\eta$. Suppose the number of signal pulses Alice emits and that of signal pulses

Bob receives are N_1 and n_1, respectively. Next, n_1 has the binomial distribution with parameters (N_1, p_1), for short,

$$n_1 \sim B(N_1, p_1). \tag{4}$$

In Ref. [32], we find N_1 is so large (typically 10^9 to 10^{10}), μ and η are approximately 10^{-2} to 10^{-1} and 10^{-4} to 10^{-3}, respectively. Thus, p_1 is roughly 10^{-6} to 10^{-4}. By the law of large numbers and the central limit theorem, when $N_1 p_1 \geq 5$ and $N_1 p_1(1-p_1) \geq 5$, the binomial distribution with parameters (N_1, p_1) can be approximately regarded as the normal distribution with mean $N_1 p_1$ and variance $N_1 p_1(1-p_1)$, given by

$$n_1 \sim N(N_1 p_1, N_1 p_1(1-p_1)). \tag{5}$$

Moreover, $p_1 \ll 1$ yields that

$$n_1 \sim N(N_1 p_1, N_1 p_1). \tag{6}$$

After standardization, we have a random variable X_1 which obeys the standard normal distribution, that is,

$$X_1 = \frac{n_1 - N_1 p_1}{\sqrt{N_1 p_1}} \sim N(0,1). \tag{7}$$

Since the only difference between the signal source and the decoy source is their intensities, it is easy to get the other random variable X_2 by analogy, denoted by

$$X_2 = \frac{n_2 - N_2 p_2}{\sqrt{N_2 p_2}} \sim N(0,1), \tag{8}$$

where N_2 and n_2 are the number of the decoy pulses Alice emits and that of the decoy pulses Bob receives, respectively. p_2 represents the probability of receiving a decoy pulse (at Bob's side) after Alice emits a decoy pulse, no matter how many photons which contains and the value of p_2 is $\nu\eta$. According to the definition of t distribution, let the random variable $Y = X_1/X_2$, then Y obeys the t distribution with a single degree of freedom, which is equivalent to the standard Cauchy distribution, that is,

$$Y = \frac{n_1/\eta - N_1\mu}{n_2/\eta - N_2\nu}\sqrt{\frac{N_2\nu}{N_1\mu}} \sim C(1,0), \tag{9}$$

where C represents the Cauchy distribution, the scale parameter is 1 and the location parameter is 0. Moreover, $\Phi(y)$ is the distribution function of Y, given by

$$\Phi(y) = \int_{-\infty}^{y} \frac{1}{\pi(1+t^2)}\mathrm{d}t, \quad -\infty < y < \infty, \tag{10}$$

where y is the value of Y and is also the test statistic that we find.

Find the value of the test statistic Set the parameters μ, ν, N_1, N_2, and η, then record n_1 and n_2. Substituting these data into Eq. (9), the desired value of the test statistic y can be obtained.

Choose a significance level We need to determine a significance level (typically 0.05) for the first test. In terms of the null hypothesis of the first test H_{o1}, we deduce that the first test is a two-tailed hypothesis testing. In addition, given the significance level of the first test α_1, the rejection region is $|y| \geq y_{[1-\alpha_1/2]}$ where $y_{[1-\alpha_1/2]}$ can be obtained by Eq. (10). More precisely, the variables $-y_{[1-\alpha_1/2]}$ and $y_{[1-\alpha_1/2]}$ refer to the boundary values between the rejection region and the acceptance region for the first test. Let the left side of Eq. (10) is equal to $\alpha_1/2$, then the upper limit of the integral will be $-y_{[1-\alpha_1/2]}$. According to the symmetry of the probability density function of the Cauchy distribution, $y_{[1-\alpha_1/2]}$ can be obtained.

Make a decision Compare the test statistic y with the critical values $y_{[1-\alpha_1/2]}$ and $-y_{[1-\alpha_1/2]}$. If $y > y_{[1-\alpha_1/2]}$ or $y < -y_{[1-\alpha_1/2]}$, we will reject H_{o1} and accept H_{a1}. This means that we believe there is a weaker version of PNS attack on the channel. Otherwise, we fail to reject H_{o1}. That is to say, we consider there is no weaker version of PNS attack on the channel. Remark the significance level of the first test α_1 is also the type I error probability of the first test, namely, the probability of mistaking no PNS attack for having a PNS attack. Let β denote the type II error probability of the first test, to be precise, the probability of mistaking having a PNS attack for no PNS attack. Note that β is usually difficult to find in most situations. Furthermore, the necessary condition for controlling the type II error probability is to demarcate the distribution type of the aggressive behavior.

2.2. The second test

The interpretation of empirical results can be conducted in any number of ways. Two approaches NIST adopted include (1) the examination of the proportion of passing the first test and (2) the distribution of P-values to check for uniformity. We adopt the first approach of NIST, which considers the empirical results of the first test and calculates the passing proportion of the first test. In this part, given the significance level of the first test α_1 and the number of the first test m, we account for the empirical results to check the correctness of the first test via the NIST Statistical Test Suite, according to illustrating the reasonability of the counting rate of accepting H_{o1}, which is called the second test in this paper. The specific analysis is as follows. Given the significance level of the second test, if the passing proportion of the first test passes the second test, the first test is proved to be correct; otherwise, the first test is proved to be wrong. The second test also contains five steps.

Identify null and alternative hypothesis Under the significance level of the first test α_1 and the number of the first

test m, let us consider the hypothesis testing problem about the null hypothesis H_{o2}: the counting rate of accepting H_{o1} with the first test is reasonable and the alternative hypothesis H_{a2}: the counting rate of accepting H_{o1} with the first test is unreasonable.

Construct the test statistic Supposing that each first test is independent and identically distributed, the confidence level of the first test is $q = 1-\alpha_1$. Let us consider further about the first test. The results contain two cases, namely, accepting H_{o1} or rejecting H_{o1}. Thereby, one can regard each first test as a Bernoulli trial. Note that the probability of accepting H_{o1} is q. Suppose the number of the first test and that of accepting H_{o1} are m and ξ, respectively. m is the times that the first hypothesis testing procedure is repeated. The value of m is set by the experimenter himself. If the experimental conditions permit (i.e., a fast enough repetition rates), the larger the value of m, the better the result. ξ refers to the times of accepting hypothesis H_{o1} when we repeat the first test m times. That is to say, for each first test executed, if the test result is accepting hypothesis H_{o1}, the value of ξ will be increased by one. Then, ξ will obey the binomial distribution with parameters (m,q), for short,

$$\xi \sim B(m,q). \tag{11}$$

When $mq \geq 5$ and $mq(1-q) \geq 5$, by the law of large numbers and the central limit theorem, the binomial distribution with parameters (m,q) can be approximatively regarded as the normal distribution with mean mq and variance $mq(1-q)$, written as

$$\xi \sim N(mq, mq(1-q)). \tag{12}$$

After standardization, we get a random variable Z which obeys the standard normal distribution, that is,

$$Z = \frac{\xi - mq}{\sqrt{mq(1-q)}} \sim N(0,1). \tag{13}$$

Furthermore, $\Psi(z)$ is the distribution function of Z, given by

$$\Psi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} \mathrm{e}^{-\frac{t^2}{2}} \mathrm{d}t, \quad -\infty < z < \infty, \tag{14}$$

where z is the value of Z and is just the test statistic that we find.

Find the value of the test statistic Select m and record ξ. Substituting these data into Eq. (13), one can get the value of the test statistic z.

Choose a significance level We need to choose a significance level α_2 (typically, $\alpha_1 = \alpha_2$) for the second test. According to the null hypothesis of the second test H_{o2}, we deduce that the second test is a two-tailed hypothesis testing. The rejection region of the second test is $|z| \geq z_{[1-\alpha_2/2]}$ where $z_{[1-\alpha_2/2]}$ can be obtained by Eq. (14). More precisely, the variables $-z_{[1-\alpha_2/2]}$ and $z_{[1-\alpha_2/2]}$ refer to the boundary values between the rejection region and the acceptance region for the second test. Let the left side of Eq. (14) be equal to $\alpha_2/2$, the upper limit of the integral will be $-z_{[1-\alpha_2/2]}$. According to the symmetry of the probability density function of the normal distribution, $z_{[1-\alpha_2/2]}$ can be obtained.

Make a decision Compare the test statistic z with the critical values $z_{[1-\alpha_2/2]}$ and $-z_{[1-\alpha_2/2]}$. If $z > z_{[1-\alpha_2/2]}$ or $z < -z_{[1-\alpha_2/2]}$, we will reject H_{o2} and accept H_{a2}. In other words, we consider the counting rate of accepting H_{o1} is unreasonable. Otherwise, we fail to reject H_{o2}. This means that we believe the counting rate of accepting H_{o1} is reasonable, and verifies the correctness of the first test at the same time.

If the result is judged to be an attack, the lower bound of Q_1 and the upper bound of e_1 will be estimated by the existing decoy-state method, and then the secure key rate will be calculated by Eq. (1). If the result is no attack, then the pulses with the same basis received including both single-photon pulses and multiphoton pulses, can be used to generate the keys. Under the assumption that the bit error is equal to the phase error even for multiphoton pulses, the secure key rate formula Eq. (1) becomes

$$R \geq qQ_\mu[1 - f(E_\mu)H_2(E_\mu) - H_2(E_\mu)]. \tag{15}$$

By comparing Eqs. (1) and (15), we can easily see the improvement of the secure key rate.

3. Experiments and analysis

In the preceding section, we show the details of our detection method. Now, we move forward to the corresponding experiments based on the aforementioned method and analyze the experimental results. The experimental setup is based on the platform of polarization encoding decoy-state BB84 implementation, with commercial compact devices at 625 MHz clock rate,[40,41] with some different parameters such as the wavelength and mean photon numbers. The mean photon numbers of the signal state and decoy state are typical around 0.4 and 0.1, respectively.[42] The block size for parameter estimation is set to 500 kbits to guarantee the freshness of final keys.[41,43] Meanwhile, η is set to a typical value 10^{-3}, which contains a typical detection efficiency of 10% and a transmittance of 1% with a 100 km-length fiber.[40]

3.1. The first test

The experimental parameters and their corresponding values of the first test are listed in Table 1. After calculation, we obtain the value of the test statistic $y = 4.90$. When the significance level of the first test $\alpha_1 = 0.05$, the critical values are $y_{[1-\alpha_1/2]} = 12.71$ and $-y_{[1-\alpha_1/2]} = -12.71$. Due to $-12.71 < 4.90 < 12.71$, the test statistic does not fall inside the rejection region and we fail to reject H_{o1}. In other words, we infer that there is no weaker version of PNS attack on the channel and the probability of being wrong is no more than 5%. The schematic diagram of the first test is illustrated in Fig. 1.

Table 1. Experimental parameters and their corresponding values of the first test.

μ	ν	N_1	N_2	n_1	n_2	η	α_1	$\lvert y_{[1-\alpha_1/2]}\rvert$	y
0.4	0.1	4.212×10^9	7.020×10^8	5.5×10^5	2.2×10^4	10^{-3}	0.05	12.71	4.90

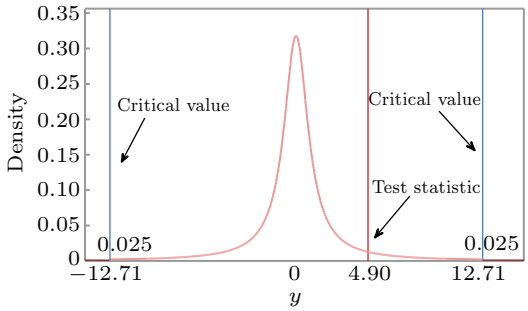


Fig. 1. The schematic diagram of the first test. The value of the test statistic y is 4.90. Given the significance level of the first test $\alpha_1 = 0.05$, the critical values are $y_{[1-\alpha_1/2]} = 12.71$ and $-y_{[1-\alpha_1/2]} = -12.71$.

3.2. The second test

In this part, we interpret the empirical results to check the correctness of the first test via the NIST Statistical Test Suite. The number of the first test and that of accepting H_{o1} are $m = 984$ and $\xi = 945$, respectively. The experimental parameters and their corresponding values of the second test are listed in Table 2. In practical QKD systems, one cannot accurately control the number of signal pulses Alice emits N_1 and that of decoy pulses Alice emits N_2. Fortunately, although the values of N_1 for each first test are not completely identical, they are very close and have the same order of magnitude. For simplicity, we ignore the effect of the minimal deviation of different N_1 and take the same strategy to N_2.

After calculation, we obtain the value of the test statistic $z = 1.49$. Given the significance level of the second test $\alpha_2 = 0.05$, the critical values are $z_{[1-\alpha_2/2]} = 1.96$ and $-z_{[1-\alpha_2/2]} = -1.96$. Since $-1.96 < 1.49 < 1.96$, the test statistic does not fall inside the rejection region and we fail to reject H_{o2}. This means that the counting rate of accepting H_{o1} is reasonable, and also further affirms the correctness of our method. That is to say, under the null hypothesis of no weaker version of PNS attack, we can judge there is no weaker version of PNS attack on the channel with an error probability of less than 5%. And then we can use Eq. (15) to calculate the secure key rate. The schematic diagram of the second test is illustrated in Fig. 2.

Table 2. Experimental parameters and their corresponding values of the second test.

μ	ν	N_1	N_2	n_1	n_2	η	m	ξ	α_2	$\lvert z_{[1-\alpha_2/2]}\rvert$	z
0.4	0.1	4.212×10^9	7.020×10^8	5.1×10^5 to 5.7×10^5	2.1×10^4 to 2.4×10^4	10^{-3}	984	945	0.05	1.96	1.49

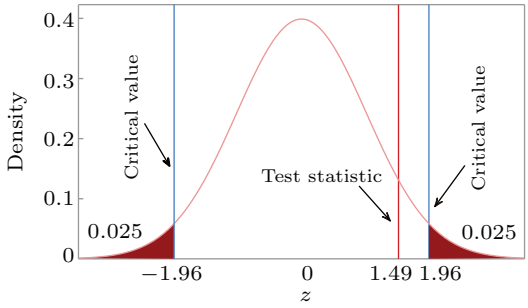


Fig. 2. The schematic diagram of the second test. The value of the test statistic z is 1.49. Given the significance level of the second test $\alpha_2 = 0.05$, the critical values are $z_{[1-\alpha_2/2]} = 1.96$ and $-z_{[1-\alpha_2/2]} = -1.96$.

4. Conclusion and discussion

In summary, we first recover the lost information of the existing decoy-state protocols when detecting the type of PNS attack which significantly changes the observed values of Alice and Bob, and extract out a Cauchy distribution statistic. Based on this information, we propose a new detection method including the first test and the second test. Most importantly, the error probability of detection can be precisely calculated in our method and we also give the calculations. Finally, according to the judgment result, we give the corresponding secure key rate. In particular, compared with the existing decoy-state protocols, the secure key rate with our method has a great improvement if the judgment result is no attack. Meanwhile, the associated experiments we performed also verify the correctness of our scheme. Nevertheless, all judgment results in this paper are obtained under the condition that the null hypothesis is no weaker version of PNS attack, which significantly changes the observed values of legitimate users. In other words, the gain of signal state or decoy state will change significantly after the type of PNS attack.[13–15,29] However, we can do nothing about stronger PNS attacks that retain the gain of signal state and decoy state, such as partial PNS attacks,[30] because the premise of the derivation no longer holds, and the type II error probability of our method in this case will be insufferable even close to unity. It should be noted that the ultimate goal of this line of research is to confirm that there are no all types of PNS attacks. For this reason, compared with the existing decoy-state methods[31–33] to directly estimate the secure key rate, our method is not yet able to be directly applied in practice now. But at least we give a new idea to detect the type of PNS attack which significantly changes the observed values of legitimate users, and improve the secure key rate and efficiency.

As for future work, one direction is to extend our ap-

proach to resist stronger version of PNS attacks.[30] In addition, in the absence of weaker version of PNS attack, since the distribution of the photon numbers received by Bob is approximated with a normal distribution, except that the ratio of two independent random variables obeying the standard normal distribution obeys a Cauchy distribution used in the paper, we can also use the conclusion that the sum of n independent random variables obeying the normal distribution still obeys a normal distribution or that the sum of squares of n independent random variables obeying the standard normal distribution still obeys a chi-square distribution of n degrees of freedom, to determine whether there is an attack and to calculate the type I error probability. It can be seen from the above analysis that our method can also be applied to other protocols containing more than one decoy state. Therefore, the other direction is to extend our method to other decoy-state QKD protocols, such as three different intensities of coherent photon source[36,44,45] and four different intensities of coherent photon source.[35]

References

[1] Bennett C H and Brassard G 2014 *Theor. Comput. Sci.* **560** 7
[2] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[4] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 080501
[5] Gisin N and Thew R 2007 *Nat. Photon.* **1** 165
[6] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[7] Duěk M, Lütkenhaus N and Hendrych M 2006 *Prog. Opt.* **49** 381
[8] Wootters W K and Zurek W H 1982 *Nature* **299** 802
[9] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818
[10] Lo H K and Chau H F 1999 *Science* **283** 2050
[11] Mayers D 2001 *J. ACM* **48** 351
[12] Renner R 2008 *Int. J. Quantum Inf.* **6** 1
[13] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev. A* **51** 1863
[14] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[15] Lütkenhaus N 2000 *Phys. Rev. A* **61** 052304
[16] Lütkenhaus N and Jahma M 2002 *New J. Phys.* **4** 44
[17] Acín A, Gisin N and Scarani V 2004 *Phys. Rev. A* **69** 012309
[18] Scarani V, Acín A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[19] Tamaki K and Lo H K 2006 *Phys. Rev. A* **73** 010302
[20] Mizutani A, Tamaki K, Ikuta R, Yamamoto T and Imoto N 2014 *Sci. Rep.* **4** 5236
[21] Yin H L, Fu Y, Mao Y and Chen Z B 2016 *Sci. Rep.* **6** 29482
[22] Lu Y S, Cao X Y, Weng C X, Gu J, Xie Y M, Zhou M G, Yin H L and Chen Z B 2021 *Opt. Express* **29** 10162
[23] Inoue K, Waks E and Yamamoto Y 2003 *Phys. Rev. A* **68** 022317
[24] Sasaki T, Yamamoto Y and Koashi M 2014 *Nature* **509** 475
[25] Yin H L, Fu Y, Mao Y and Chen Z B 2016 *Phys. Rev. A* **93** 022330
[26] Gu J, Cao X Y, Yin H L and Chen Z B 2021 *Opt. Express* **29** 9165
[27] Korzh B, Lim C C W, Houlmann R, Gisin N, Li M J, Nolan D, Sanguinetti B, Thew R and Zbinden H 2015 *Nat. Photon.* **9** 163
[28] Cao X Y, Gu J, Lu Y S, Yin H L and Chen Z B 2021 *New J. Phys.* **23** 043002
[29] Liu W T, Sun S H, Liang L M and Yuan J M 2011 *Phys. Rev. A* **83** 042326
[30] Liu D, Wang S, Yin Z Q, Chen W and Han Z F 2013 *Chin. Sci. Bull.* **58** 3859
[31] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[32] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[33] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[34] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Info. Comput.* **4** 325
[35] Wang X B 2005 *Phys. Rev. A* **72** 012322
[36] Yu Z W, Zhou Y H and Wang X B 2015 *Phys. Rev. A* **91** 032318
[37] Zhou Y H, Yu Z W, and Wang X B 2016 *Phys. Rev. A* **93** 042324
[38] Wang X B, Yu Z W, and Hu X L 2018 *Phys. Rev. A* **98** 062323
[39] Bassham L, Rukhin A, Soto J, Nechvatal J, Smid M, Leigh S, Levenson M, Vangel M, Heckert N and Banks D 2010 *NIST. SP* **9** 800
[40] Wang L J, Zou K H, Sun W, Mao Y Q, Zhu Y X, Yin H L, Chen Q, Zhao Y, Zhang F, Chen T Y and Pan J 2017 *Phys. Rev. A* **95** 012301
[41] Mao Y Q, Wang B X, Zhao C X, Wang G Q and Pan J W 2018 *Opt. Express* **26** 6010
[42] Yuan Z L, Plews A, Takahashi R, Doi K, Tam W, Sharpe A W, Dixon A R, Lavelle E, Dynes J F, Murakami A, Kujiraoka M, Lucamarini M, Tanizawa Y, Sato H and Shields A J 2018 *J. Light. Technol.* **36** 3427
[43] Liu Y, Chen T Y, Wang J, Cai W Q, Wan X, Chen L K, Wang J H, Liu S B, Liang H, Yang L, Peng C Z, Chen K, Chen Z B and Pan J W 2010 *Opt. Express* **18** 8587
[44] Wang X B 2013 *Phys. Rev. A* **87** 012320
[45] Yu Z W, Zhou Y H and Wang X B 2013 *Phys. Rev. A* **88** 062339