https://doi.org/10.1140/epjqt/s40507-023-00175-0

EPJ.org

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH

Open Access

Decoy state semi-quantum key distribution

Shuang Dong[1], Shang Mi[1], Qingcheng Hou[1], Yutao Huang[1], Jindong Wang[1*], Yafei Yu[2], Zhengjun Wei[1], Zhiming Zhang[2] and Junbin Fang[3]

*Correspondence: wangjindong@m.scnu.edu.cn
[1] Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou 510006, China
Full list of author information is available at the end of the article

Abstract

Semi-quantum key distribution describes a system in which a fully quantum user and classical user perform key distribution. The main advantage of key distribution is its security. Owing to the bottlenecks of existing technology, highly attenuated lasers and threshold detectors are required for semi-quantum key distribution; however, these components make semi-quantum key distribution susceptible to eavesdroppers. Our previous study presented the first semi-quantum key distribution experiment and verified the feasibility of the mirror protocol in 2021. Herein, we first build a semi-quantum key distribution channel model and use Gottesman-Lo-Lütkenhaus-Preskill theory to evaluate its safety performance in the case of a quasi-single photon source. Moreover, we determine that an eavesdropper can steal all information through the photon-number-splitting attack without being detected. Therefore, we add decoy states to the semi-quantum key distribution to estimate the furthest transmission distance and secure bit rate under asymptotic conditions. Semi-quantum key distribution can still be achieved safely with highly attenuated lasers and threshold detectors in 150 km.

Keywords: Semi-quantum key distribution; Channel model; Photon-number-splitting attack; Decoy state

1 Introduction

Quantum key distribution (QKD) allows two quantum users, Alice and Bob, to securely share a string of keys. In theory, the distribution of secret quantum keys is unconditionally secure based on the laws of quantum physics. Its protocol [1] and its security has been fully proved. Furthermore, various experimental schemes have been proposed to demonstrate the practical feasibility of QKD [2–6]. Some state-of-the art QKD protocols, e.g. MDI-QKD and TF-QKD make the transmission distance of QKD become longer and the performance become better [7–10]. With the gradual development and maturity of practical systems, security evaluations for real systems have been gradually recognized and valued [11–13]. However, these security analyses are limited to the utilization of single-photon sources. In practice, a highly attenuated laser is used as the light source; therefore, an eavesdropper, Eve, can steal information via the photon-number-splitting (PNS) attack without being detected [14–17]. The decoy state [18–23] and SARG04 protocol [24] were successively proposed to counteract PNS attacks. Of the two, the decoy states protocol is widely used because it is more effective.

Semi-quantum key distribution (SQKD) was proposed to share keys between a quantum user and classical user. At present, there are no actual full quantum computers; thus, it is unpractical to implement the quantum communications via using fully quantum devices. And the SQKD protocol could be enabled in a limited quantum resource environment without losing their security. In 2007, Boyer, Kenigsberg, and Mor proposed a new quantum communication protocol—the semi-quantum key distribution protocol (BKM07 protocol) [25]. Subsequently, BGKM-09 [26], the less than four state protocol [27], and mirroring protocol [28] were proposed. When the design of the SQKD protocol was proposed, its theoretical security was subsequently proven, particularly for independent attacks and collective attacks [29–31]. Additionally, SQKD's security bit rate was also determined.

Our previous study presented the first SQKD experiment and verified SQKD's feasibility in 2021 [32]. However, the experiment utilized highly attenuated lasers and threshold detectors. A safety analysis of SQKD with a strongly attenuated laser has not been presented. Strongly attenuated pulses inevitably result in multi-photon pulses, which opens a door for PNS attacks. Therefore, it is necessary to determine if SQKD can resist PNS attacks. If SQKD cannot detect PNS attacks, it is important to investigate if SQKD can also use decoy state methods to make experiments more secure using essentially the same hardware. Therefore, the experimental safety of SQKD must be evaluated. These three points of investigation are essential for SQKD's development. In this study, we first build an SQKD channel model based on the BKM-07 protocol and identified that Eve can steal all information through PNS attacks without being detected. Moreover, we use Gottesman-Lo-Lütkenhaus-Preskill(GLLP) theory [33] to evaluate its safety performance when using a strongly attenuated laser. Therefore, we added decoy states to the SQKD and estimated the maximum transmission distance and secure bit rate under asymptotic conditions. Semi-quantum key distribution can still be achieved safely with highly attenuated lasers and threshold detectors in 150 km. Decoy SQKD and decoy QKD [18–22] can increase the safe transmission distance. From the perspective of scheme architecture, SQKD has two channels, so when estimating some backward channel's parameters, such as μ_2, ν_2, the length of the forward channel will be associated with μ_2, ν_2. This is the difference between SQKD decoy and QKD decoy. In the processing of the result, QKD decoy only needs $R_{qkd} > 0$. For SQKD decoy, it need $I_f > 0$, $I_b > 0$ and $R_{sqkd} > 0$. This condition limits the maximum transmission distance of SQKD.

The organization of this paper is as follows. In Sec. 2, we build an SQKD channel model and prove SQKD is not secure against PNS. Moreover, we establish the secure bit rate of SQKD with GLLP theory. In Sec. 3, we analyze several decoy states of SQKD. The results are showed and discussed in Sec. 4. In Sec. 5, we present some concluding remarks.

2 Theoretical model

The BKM-07 protocol [25] model shown in Fig. 1. The SQKD we discuss later is based on this model. We call Bob select the reflected photon CTRL, and Bob select the measured resend photon SIFT.

2.1 SQKD channel model

SQKD has two logical channels, a forward channel and back channel; however, they share the same physical channel. Bob can choose to use the SIFT operation to detect the photon using the forward channel and resend the photon to Alice through the backward channel.

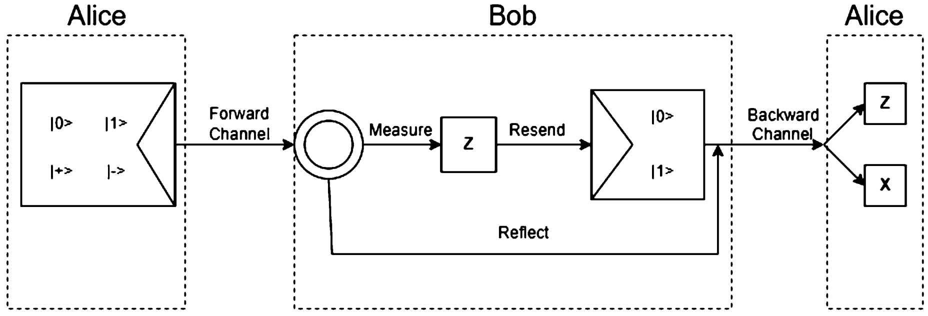

Figure 1 BKM-07 protocol model. (1) Alice generates random qubits in the Z or X bases. (2) For each qubit, Bob randomly chooses to measure Alice's qubit in the Z basis (to SIFT it) or to reflect it back (CTRL). (3) Bob may also only prepare Z basis qubits. When Bob chooses the SIFT operation, Bob resends the qubit with the same result as his measurement. (4) Alice measures each qubit using the basis she sent it in. (5) Alice publishes qubits which are her Z-basis bits, and Bob publishes qubits which he choose to SIFT

Moreover, if Bob chooses the CTRL operation to return the photon, the whole process can be viewed as Alice sending the photons and then measuring them after they are transmitted through the whole channel (forward and backward channel). Alice needs to perform both sending and receiving operations; therefore, we call the Alice of the sender as Alice and the Alice of the receiver as $Alice'$.

We start with two assumptions.

First, we assume that these two logical channels are independent when Bob chooses the SIFT operation. This assumption limits the cases in which Eve can make a joint attack on the forward and backward channels, and we will consider more complex cases in the future. In fact, the backward and forward channels are essentially the same physical channels. Thus, they are subject to the same constraints, such as losses and transmission distance ($L = L_f = L_b$).

Second, we simplify the analysis by considering $Alice'$ as the third user. In SQKD, no matter what operation Bob chooses and what state Alice sends, $Alice'$ can measure the photon based on the state of Alice. This correlation is equivalent to the fact that Alice and Bob need to have compatible bases only once. (If Alice, Bob, and $Alice'$ are independent of each other, in the absence of SQKD, two information transfers need to have compatible bases twice).

Based on the above two assumptions, the whole channel can be regarded as a cascade of the forward channel and backward channel. Moreover, the two channels are independent; therefore, the information of $Alice'$ only depends on Bob and has no direct relationship with Alice. That is, Alice, Bob, and $Alice'$ constitute a first-order Markov chain. We study this channel model to obtain a secure bit rate evaluation formula. Therefore, the following analysis is based on the case where Alice chooses to send a Z-basis state, and Bob chooses the SIFT operation. The Z-basis channel noise can be used to describe channels parameters and will lead to the generation of the quantum bit error. We let E_{BS} and E_{AS} denote the quantum bit error rate (QBER) in the Z-basis for Bob and $Alice'$, respectively. Additionally, E_{BS} and E_{AS} can be estimated from the detections made by Bob and $Alice'$, respectively.

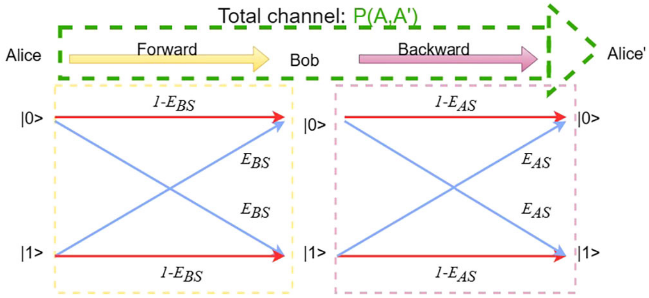

Figure 2 SQKD channel model. The yellow dotted boxes, pink dotted boxes, and green dotted boxes represent the forward, backward, and total channels, respectively; the red and blue lines denote the secure and error bits, respectively

This SQKD channel model and its parameters are shown in Fig. 2. The transition probability matrixes for the forward channel is

$$\begin{pmatrix} 1-E_{BS} & E_{BS} \\ E_{BS} & 1-E_{BS} \end{pmatrix}. \tag{1}$$

And the transition probability matrixes for the backward channel is

$$\begin{pmatrix} 1-E_{AS} & E_{AS} \\ E_{AS} & 1-E_{AS} \end{pmatrix}. \tag{2}$$

Here we emphasize that when the state sent by Alice is different from that received by $Alice'$, i.e., Alice sends $|0\rangle(|1\rangle)$ and $Alice'$ detects $|1\rangle(|0\rangle)$, such bits should be discarded in the protocol. When the state sent by Alice is the same as that detected by $Alice'$, and if Bob and $Alice'$ receive the same state, they share a bit. If Bob and $Alice'$ obtain different states, the bit is considered an error bit. The SQKD total model are shown in Fig. 2. The following matrix is the transition probability matrix of the equivalent SQKD

$$\begin{pmatrix} 1-E_{BS}-E_{AS}+2E_{BS}E_{AS} & E_{BS}-E_{AS}+2E_{BS}E_{AS} \\ E_{BS}-E_{AS}+2E_{BS}E_{AS} & 1-E_{BS}-E_{AS}+2E_{BS}E_{AS} \end{pmatrix}. \tag{3}$$

2.2 PNS in SQKD

We briefly describe the PNS attack. If a pulse does not contain photons, Eve does nothing. However, if a pulse contains a single photon, Eve blocks the single photon with probability P. If a pulse contains multiple photons, Eve can extract one of them and store it in a quantum memory, and the remaining photons will be sent back to Bob through a lossless channel. If $P > 1$, Eve may even block some of the multi-photon pulses to keep Q_μ constant.

Q_{BS} is the gain of the SIFT photons detected by Bob. Q_{AC} and Q_{AS} are the gain of the CTRL and SIFT photons detected by $Alice'$. When Eve only attacks one channel, Eve cannot keep Q_{AC} and Q_{BS} constant. Moreover, the two gains will not be equal because SIFT photons have a higher detection loss. Thus, Alice and Bob can detect anomalies.

Here, we assume that Eve's attacks on the forward and backward channels are independent, based on the first assumption. Eve attacks the forward channel first, then the backward channel. The CTRL photon goes through the forward and backward channels, whereas the SIFT photon only goes through the backward channel. Eve can block single photons and extract them out of all the multi-photon pulses in the forward channel with probability P_1. It is possible for Eve to block a single photon with probability P_2 and extract it from any multi-photon pulses in the backward channel. P_1 affects only CTRL photons, and P_2 affects SIFT and CTRL photons. Therefore, an appropriate P_1 and P_2 can always be determined to keep Q_{AC} and Q_{BS} unchanged [34].

Let the average photon number of SIFT be μ, which is also the average number of photons sent by Alice. And that of CTRL be ν, which is the average number of CTRL photons sent by Bob. Assume that Eve attacks the forward and backward channels with probabilities of P_1 and P_2, respectively.

For SIFT photons:

$$e^{-\mu}\frac{\mu^n}{n!} \to \begin{cases} e^{-\mu}(1+P_2\mu) & n=0, \\ (1-P_2)\mu e^{-\mu}+\frac{\mu^2}{2}e^{-\mu} & n=1, \\ \frac{\mu^{n+1}}{(n+1)!}e^{-\mu} & n>1. \end{cases} \tag{4}$$

For CTRL photons:

Through the forward channel, the photon number distribution is

$$e^{-\nu}\frac{\nu^n}{n!} \to \begin{cases} e^{-\nu}(1+P_1\nu) & n=0, \\ (1-P_2)\nu e^{-\nu}+\frac{\nu^2}{2}e^{-\nu} & n=1, \\ \frac{\mu^{n+1}}{(n+1)!}e^{-\nu} & n>1. \end{cases} \tag{5}$$

Through the backward channel, the photon number distribution is

$$e^{-\nu}\frac{\nu^n}{n!} \to \begin{cases} e^{-\nu}\{1+P_1\nu+P_2[(1-P_1)\nu+\frac{\nu^2}{2}]\} & n=0, \\ e^{-\nu}\{[1-P_2][(1-P_1)\nu+\frac{\nu^2}{2}]+\frac{\nu^3}{3!}\} & n=1, \\ \frac{\nu^{n+2}}{(n+2)!}e^{-\nu} & n>1. \end{cases} \tag{6}$$

Now, we assume that Eve can control the total loss inside Bob and *Alice*′; thus, $Y_n^{PNS}=1$ $(n\geq 1)$.

To keep Q_{BS} unchanged, it needs to satisfy the following: $Q_{BS}=1-\mathrm{e}^{-\eta\mu}=(1-P_2)\mu\mathrm{e}^{-\mu}+\sum_{n=2}^{\infty}\mathrm{e}^{-\mu}\frac{\mu^n}{n!}$. Then, we obtain:

$$P_2=\frac{1}{\mu}\left[e^{\mu(1-\eta)}-1\right]. \tag{7}$$

To keep Q_{AC} unchanged, it needs to satisfy the following: $Q_{AC}=1-\mathrm{e}^{-\eta\nu}=[1-P_2][(1-P_1)\nu\mathrm{e}^{-\nu}+\frac{\nu^2}{2}e^{-\nu}]+\frac{\nu^3}{3!}e^{-\nu}+\sum_{\mathrm{n}=4}^{\infty}e^{-\nu}\frac{\nu^n}{n!}$. Then, we obtain:

$$P_1=\frac{1+P_2(\nu+\frac{\nu^2}{2})-e^{\nu(1-\eta)}}{\nu(P_2-1)}. \tag{8}$$

The limiting condition is $P_2>1$. That is, Eve needs to block some multi-photon pulses to ensure a constant Q_{BS} and Q_{AC}.

Through mathematical analysis, when the average number of photons is smaller than 0.7, $P_1 > 1$. Both P_1 and P_2 are bigger than 1; thus, we believe that Eve blocks all single photons, that is, $P_1 = 1$, $P_2 = 1$, and Eve blocks two-photons from multi-photon pulses with a probability of P_3 to keep Q_{BS}. And Eve blocks three-photons from multi-photon pulses with a probability of P_4 to keep Q_{AC} unchanged.

We can get the distribution

$$e^{-\mu}\frac{\mu^n}{n!}\begin{cases} e^{-\mu}(1+\mu+P_3\frac{\mu^2}{2}) & n=0, \\ e^{-\mu}(1-P_3)\frac{\mu^2}{2} & n=1, \\ \frac{\mu^{n+1}}{(n+1)!}e^{-\mu} & n>1. \end{cases} \tag{9}$$

To keep Q_{BS} unchanged, we obtain

$$P_3 = \frac{2[(e^{\mu(1-\eta)} - 1 - \mu]}{\mu^2}. \tag{10}$$

Through the backward channel, the photon number distribution is

$$e^{-\nu}\frac{\nu^n}{n!}\begin{cases} e^{-\nu}(1+\nu+\frac{\nu^2}{2}+P_4\frac{\nu^3}{3!}) & n=0, \\ e^{-\nu}(1-P_4)\frac{\nu^3}{3!} & n=1, \\ \frac{\nu^{n+2}}{(n+2)!}e^{-\nu} & n>1. \end{cases} \tag{11}$$

To keep Q_ν unchanged, we can get

$$P_4 = \frac{6(e^{\nu(1-\eta)} - 1 - \nu - \frac{\nu^2}{2})}{\nu^3}. \tag{12}$$

Eve can block all single photons and some photons from multi-photon pulses to keep Q_{BS} and Q_{AC} unchanged. In conclusion, SQKD is not secure against PNS attacks.

2.3 The secure bit rate of SQKD with GLLP theory

According to the Csiszár–Körner theory [35], the lower bound of a QKD system secure bit rate is equal to the mutual information between Alice and Bob($I(A;B)$) minus the mutual information between Eve and Bob (or Alice). Because reverse data reconciliation is adopted in QKD, the lower bound of the secure bit rate is: $R = I(A;B)_{QKD} - I(A;E)_{QKD}$.

The mutual information between Alice and Bob and $Alice'$ is $I(A;A')$. Reverse data reconciliation is also adopted in SQKD; therefore, the lower bound of the secure bit rate is: $R = I(A;A') - I(A;E)$.

According to the Shor-Preskill theory [36], $I(A;B) = qQ_\mu[1 - H_2(E_\mu)]$, where Q_μ and E_μ are the gain and QBER of the QKD, respectively, and H_2 is the binary Shannon entropy. $E_\mu = \frac{e_0 Y_0 + e_{\text{det}}(1-e^{-\eta\mu})}{Q_\mu}$, where, e_0 is the secret number of zero photon signal. e_{det} is the bit error rate of the system optical path. In SQKD, the QBER should be corrected to $E_{BS} + E_{AS} - 2E_{BS}E_{AS}$ through the channel model; $I(A;E) = q(Q_1 H_2(e_1) + Q_\mu - Q_0 - Q_1)$, where Q_1 is the single photon error rate. The QBER requires further discussion for SQKD.

In SQKD, we can get experimental data Q_{BS} and Q_A, where Q_{BS} and Q_A are the gains of Bob and $Alice'$, respectively. When Alice sent a Poisson source with an average number of photons μ_1, $Q_{BS} = Y_0 + 1 - e^{-\eta\mu_1}$, where Y_0 is the gain of dark count. $Y_0 \approx 2p_d$, where p_d is the secret count rate of a detector. η is the forward channel transmittance of a single photon signal. $\eta = 10^{-\alpha L/10}\eta_{\mathrm{b}}\eta_d$, where η_d is the detection efficiency, η_b is the transmittance of Bob. $Q_A = Q_{AS} + Q_{AC}$, where Q_{AS} and Q_{AC} are the gains when Bob choose SIFT and CTRL operations. When Bob resent a Poisson source with an average number of photons μ_3, $Q_{AS} = Y_0 + 1 - e^{-\eta\mu_3}$. The CTRL photons through total channel sent by Alice: $Q_{AC} = Y_0 + 1 - e^{-2\eta\mu_1}$. We can divide Q_A into Q_{AS} and Q_{AC} through Alice publishes which were her Z bits and Bob publishes which ones he chose to SIFT.

We first analyze $I(A;A')$. When the detectors of $Alice'$ and Bob do not respond or their bases are incompatible, there is no correlation between the measurement result obtained by $Alice'$ and the state sent by Alice. In this case, $I(A;A') = 0$. When the detectors of $Alice'$ and Bob respond and their measurement bases are in agreement, the measurement result can share a sifted bit. In this case,

$$I\bigl(A;A'\bigr) = qQ_{AS}Q_{BS}\bigl[1 - H_2(E_{BS} + E_{AS} - 2E_{BS}E_{AS})\bigr], \tag{13}$$

where q is the probability that Alice sends a Z-basis ($q = 1/2$).

Eve needs to attack both channels to obtain more information. Based on our second assumption, we now suggest that Eve attacks independently in the forward and backward channels. According to the Shor-Preskill theory, Eve can extract all the information from multi-photon pulses. At this stage, the transmission channel is equivalent to a noiseless lossless channel for Bob and $Alice'$. When single-photon pulses are received, Eve can also steal information. However, for Bob and $Alice'$, the transmission channel is equivalent to a binary symmetric channel, such as the SQKD model that we previously built; the channel parameter is the QBER of the single-photon pulses.

When both $Alice'$ and Bob respond with single-photon pulses, the channel is equivalent to two binary symmetric channels in series. The amount of information obtained by Eve is as follows:

$$I(A;E) = qQ_{AS1}Q_{BS1}H_2(e_{BS1} + e_{AS1} - 2e_{BS1}e_{AS1}), \tag{14}$$

where Q_{BS1} and Q_{AS1} are the gains of Bob and $Alice'$ for single-photon pulses, respectively, and e_{BS1} and e_{AS1} are the QBERs of Bob and $Alice'$'s SIFT part for single-photon pulses, respectively.

When the responses of Bob and $Alice'$ are a single photon and multiple photons, respectively, the channel is equivalent to a binary symmetric channel and a noiseless lossless channel in series. Moreover, the amount of information obtained by Eve is as follows

$$I(A;E) = qQ_{BS1}Q_{ASm}H_2(\mathrm{e}_{BS1}), \tag{15}$$

where Q_{ASm} is the multi-photon response rate of $Alice'$'s SIFT part.

When Bob has a multi-photon response and $Alice'$ a single photon, the channel is equivalent to a binary symmetric channel and noiseless lossless channel in series. Moreover, the amount of information obtained by Eve is as follows:

$$I(A;E) = qQ_{BSm}Q_{AS1}H_2(\mathrm{e}_{AS1}), \tag{16}$$

where Q_{BSm} is Bob's gain of the multi-photon pulses.

When both $Alice'$ and Bob's responses are multi-photon pulses, the channel is equivalent to two noiseless lossless channels in series. Then, the amount of information obtained by Eve is as follows:

$$I(A;E) = qQ_{BSm}Q_{ASm}. \tag{17}$$

In other cases, $I(A;E) = 0$.

In the case of $Q_0 = 0$, Eve has the highest advantage. At this time, the security bit rate of SQKD is as follows:

$$\begin{aligned} R = qQ_{AS}Q_{BS}\{&-H_2(E_{BS} + E_{AS} - 2E_{BS}E_{AS}) \\ &+ \Delta_B[1 - H_2(e_{BS1})] + \Delta_A[1 - H_2(e_{AS1})] \\ &- \Delta_A\Delta_B[1 - H_2(e_{BS1}) - H_2(e_{AS1}) + H_2(e_{BS1} + e_{AS1} - 2e_{BS1}e_{AS1})]\}, \end{aligned} \tag{18}$$

where q is the probability that Alice sends a Z-basis ($q = 1/2$), $\Delta_B = \frac{Q_{BS1}}{Q_{BS}}$, $\Delta_A = \frac{Q_{AS1}}{Q_{AS}}$.

It can be observed from Eq. (18) that the parameters we need to estimate are Q_{AS1}, e_{AS1}, Q_{BS1}, and e_{BS1}. The GLLP theory uses two worst-case assumptions to estimate these parameters. The first assumption is that all the multi-photon pulses are detected: $Q_{BS1} = Q_{BS} - P_{mA}$, $Q_{AS1} = Q_{BS} - P_{mB}$, where P_{mA} and P_{mB} are the probability that Alice and Bob send multiple photons, respectively. The second assumption is that the multi-photon pulses do not introduce an error rate: $e_{BS1} = \frac{E_{BS}}{\Delta_B}$, $e_{AS1} = \frac{E_{AS}}{\Delta_A}$. We construct the secure bit rate through the whole channel.

Additionally, we can analyze forward and backward channels separately using the GLLP theory. It is important to note that the analysis of forward and backward channels can only estimate the longest SQKD transmission distance. Eq. (19) and Eq. (20) denote the mutual information of the forward and backward channels, respectively:

$$I_f = qQ_{BS}\left\{-H_2(E_{BS}) + \frac{Q_{BS1}}{Q_{BS}}[1 - H_2(\mathrm{e}_{BS1})]\right\}, \tag{19}$$

$$I_b = qQ_{AS}\left\{-H_2(E_{AS}) + \frac{Q_{AS1}}{Q_{AS}}[1 - H_2(\mathrm{e}_{AS1})]\right\}. \tag{20}$$

We need to estimate the theoretical values of Q_μ and E_μ, so we need to set some parameters. We set $\eta_d = 0.15$ and $p_d = 2 * 10^{-6}$; $e_{\mathrm{det}} = 0.01$; $\eta_b = 0.4$. The results are shown in Fig. 3(a). The longest transmission distance estimated using the SQKD secure bit rate can reach 8 km, which is the same as the QKD transmission distance under the same conditions. The maximal distance of forward and backward channel are 16 km and 2 km, respectively. Obviously, since the average number of photons transmitted in the backward channel is smaller than that transmitted in the forward channel, the transmission distance in the forward channel is larger than that in the backward channel when the furthest transmission distance in the forward channel is calculated independently. To ensure the safety of any channel, the actual longest distance is limited to the shortest distance out of the three lengths. Therefore, the longest distance should be 2 km. It is the same as the QKD transmission distance when the $\mu = 0.1$. The security bit rate of SQKD depends on the soild blue line.

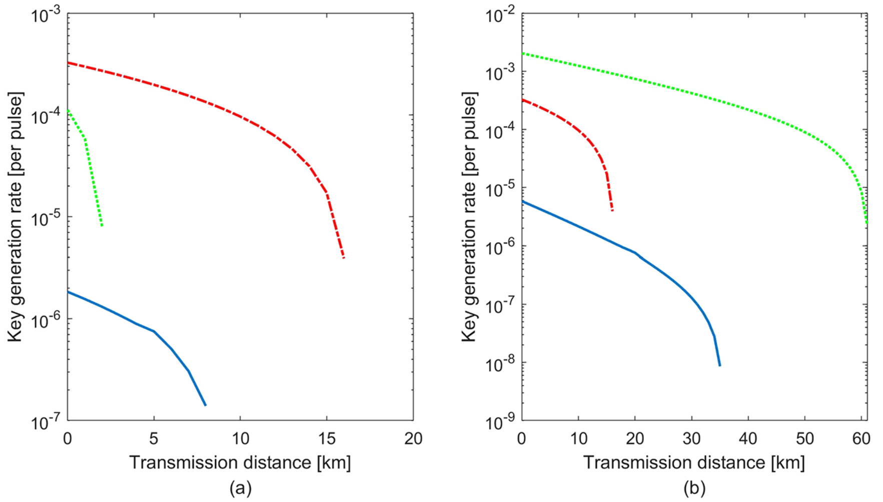

Figure 3 (**a**) secure bit rate with GLLP theory. (**b**) secure bit rate with backward channel has decoy state. The dashed line shows the performance of the forward channel with Alice transmitting $\mu_1 = 0.05$. The dotted line shows the performance of the backward channel with Bob transmitting $\mu_3 = 0.1$. The solid line shows the SQKD secure bit with $\mu_1 = 0.05$ and $\mu_3 = 0.1$

3 Analysis

3.1 Decoy state in backward channel

In reality, the photon-number distribution of a strongly attenuated source follows a Poisson distribution with a small average number of photons. In the above analysis, we ignore the average number of photons that Bob resends. The following describes the constraints on Bob when resending photons.

Suppose the average number of photons sent by Alice is μ_1, and the average number of photons sent by Bob is μ_3.

We use η to describe the channel loss. After the channel loss, the average number of photons that reaches Bob decreases to μ_2, $\mu_2 = \eta\mu_1$. Moreover, the Poisson distribution of photons is

$$P_{\text{loss}}[n] = \frac{(\eta\mu_1)^n}{n!} e^{-\eta\mu_1}. \tag{21}$$

If Bob chooses the SIFT operation, the SIFT operation will cause a measurement loss η_{det}. Then, after the channel loss and detection loss are accounted for, the Poisson distribution of Bob's transmission is

$$P_{\text{det}}[n] = \frac{(\eta_{\text{det}}\eta\mu_1)^n}{n!} e^{-\eta_{\text{det}}\eta\mu_1}. \tag{22}$$

We should first ensure that $P_{\text{loss}}[n] \geq P_{\text{det}}[n]$. Bob can control the corresponding part of a pulse and separate it to send an empty pulse; therefore, he can ensure $P_{\text{loss}}[0] = P_{\text{det}}[0]$. However, $P_{\text{loss}}[0] = e^{-\eta\mu_1} \leq e^{-\eta_{\text{det}}\eta\mu_1} = P_{\text{det}}[0]$, $0 < \eta_{\text{det}} \leq 1$.

Therefore, although Bob can control the photon-number distribution, he cannot transmit a Poisson distribution that is the same as the CTRL average number of photons. Bob can only transmit Poisson distributions with a smaller average number of photons. That is, the number of photons that are resent is $\mu_2 < \eta_{\text{det}}\eta\mu_1$.

In the above analysis, we assumed that Bob can control the photon-number distribution. However, such an assumption is meaningless because current technology cannot achieve this condition.

Here, we propose a solution: Bob still emits a Poisson distribution with an average photon number of μ_2 whether Bob is unresponsive or detected. Although there is no response to Bob, Bob just attaches polarization information ($|0\rangle$ or $|1\rangle$) to the photon. Thus, Bob can send a Poisson distribution with an average photon number that is fully μ_2. Moreover, it can be significantly greater than $\eta\mu_1$ to increase the signal-to-noise ratio (SNR). In the actual key-distribution process, after confirming basis compatibility, Alice and Bob can conduct error-code detection. If the error code detection is verified, Bob can announce which bits were unresponsive so that secure bits can be formed between Alice and Bob.

In addition, we can make the average number of CTRL photons different from that of SIFT photons so that we can create a decoy state in the backward channel. We add decoy state to accurately estimate Q_{AS1} and e_{AS1}. he result is shown in Fig. 3(b). The longest transmission distance estimated using the SQKD secure bit rate can reach 35 km. The maximal distance of forward channel is 16 km. The maximal distance of backward channel is 61 km. Although the furthest distance of the backward channel is estimated to be longer, the longest SQKD distance is determined using the shortest of the three distances. Therefore, the longest SQKD transmission distance can be increased to 16 km only by adding decoy states to the backward channel.

3.2 Setting decoy states

Based on the previous analysis of PNS attacks, the forward channel is less secure than the backward channel. Adding decoy states to Alice is equivalent to adding decoy states to the whole channel. First, we consider the case where Alice sends the signal state and decoy states with different average photon numbers, that is, μ_1 and ν_1, respectively. This ensures that the forward channel is capable of detecting PNS attacks. Then, Bob resends the signal states with an average photon number of μ_3. We scan μ_3, μ_1, ν_1 from 0.1 to 1.0 in step size 0.01 to find the maximum bit rate for each 10 km to 130 km. We chose to be under $\mu_3 > \mu_1 > \nu_1$ conditions [21]. The result shows in Table 1. We set $\mu_1 = 0.36$;

Table 1 Set the average number of photons per 10 km at the highest secure bit rate

L	R	μ_3	μ_1	ν_1	l_f	l_b
0	0.000196962	0.68	0.36	0.08	0.004545272	0.004033408
10	7.84286E–05	0.68	0.36	0.08	0.002855023	0.0024813
20	3.1182E–05	0.68	0.36	0.08	0.00179378	0.001538292
30	1.2376E–05	0.68	0.36	0.08	0.001126285	0.00095793
40	4.90028E–06	0.68	0.36	0.08	0.000705973	0.00059759
50	1.93333E–06	0.68	0.36	0.08	0.000441124	0.000372548
60	7.58502E–07	0.68	0.36	0.08	0.000274173	0.000231472
70	2.94926E–07	0.68	0.36	0.08	0.000168923	0.000142828
80	1.13013E–07	0.68	0.36	0.08	0.000102589	8.70607E–05
90	4.2264E–08	0.68	0.36	0.08	6.08191E–05	5.19701E–05
100	1.51578E–08	0.68	0.35	0.08	3.44918E–05	3.18463E–05
110	5.05688E–09	0.68	0.34	0.09	1.88718E–05	1.6531E–05
120	1.46186E–09	0.68	0.31	0.1	8.95178E–06	8.90369E–06
130	2.8517E–10	0.68	0.27	0.11	2.96385E–06	4.26817E–06

$\nu_1 = 0.08$; and $\mu_3 = 0.68$. In the one decoy state, estimation of Y_1 is:

$$Y_{1_{one}} = \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - \frac{\nu^2}{\mu^2}Q_\mu e^\mu - \frac{\mu^2 - \nu^2}{\mu^2}\frac{E_\mu Q_\mu e^\mu}{e_0}\right). \tag{23}$$

And the estimation of e_1 is:

$$e_{1_{one}} = \frac{E_\mu Q_\mu e^\mu - E_\nu Q_\nu e^\nu}{Y_1(\mu - \nu)}. \tag{24}$$

3.2.1 *The average number of photons in a signal state resent by Bob*

After the above discussion, Bob resends a Poisson distribution with an average photon number of μ_3 for all photons (with and without responses), where μ_3 can have an arbitrary value.

At the time when the photon sent from Alice reaches Bob, the average number of photons is $\mu_2(\nu_2)$, $\mu_2(\nu_2) = \eta\mu_1(\nu_1)$.

If $\mu_3 = \mu_2$, Bob should resend photons that are physically related to the forward channel using the same average photon number. The resent photons in the backward channel have their own losses in the forward channel, but in this way, the backward channel has only one decoy state. Figure 4 shows that the furthest transmission distance reaches 84 km because the decoy state is added.

If $\mu_3 > \mu_2 > \nu_2$, the larger average photon number μ_3 of the signal-state can result in a two decoy states in the backward channel. Moreover, it can increase the SNR and secure bit rate.

The result in Fig. 5(a) shows that adding decoy states to Alice increases the SQKD transmission distance up to 140 km. The maximal distance of forward channel is 134 km. The maximal distance of backward channel is 155 km. This shows that adding one decoy state

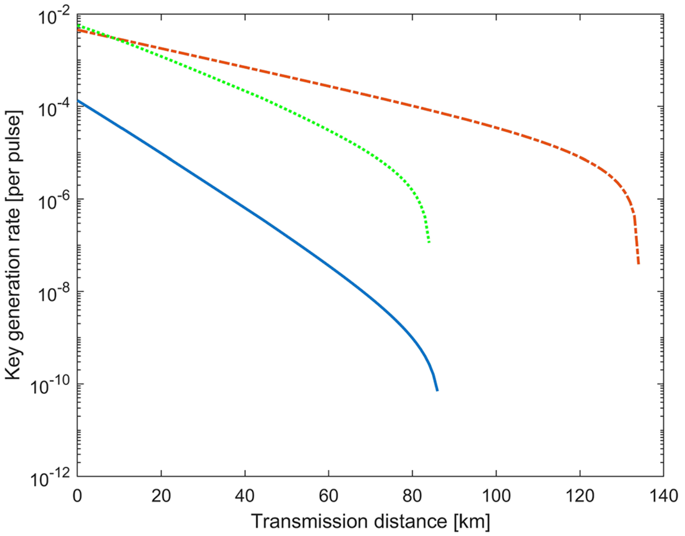

Figure 4 $\mu_3 = \mu_2$ in backward the channel. The dashed red line shows the performance of the forward channel with Alice transmitting $\mu_1 = 0.36$. Its maximal distance is 134 km. The dotted green line shows the performance of the backward channel with Bob transmitting $\mu_3 = \mu_2$. Its maximal distance is 84 km. The solid blue line shows the SQKD secure bit with $\mu_1 = 0.36$ and $\mu_3 = \mu_2$. Its maximal distance is 86 km. Therefore, the SQKD transmission distance is 84 km

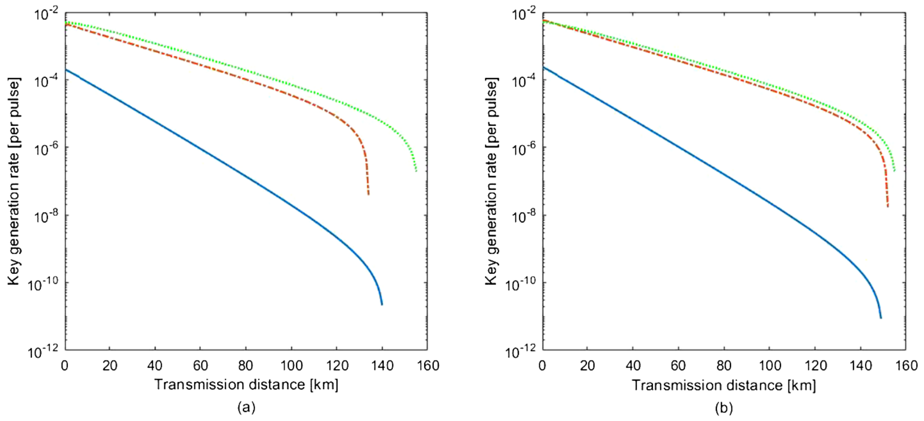

Figure 5 (**a**) Adding one decoy state. (**b**) Adding two decoy states. The dashed red line shows the performance of the forward channel with Alice transmitting $\mu_1 = 0.36$. The dotted green line shows the performance of the backward channel with Bob transmitting $\mu_3 = 0.68$. The solid blue line shows the SQKD secure bit with $\mu_1 = 0.36$ and $\mu_3 = 0.68$

to the forward channel can increase the transmission distance of the forward channel and enable the backward channel to add two decoy states to increase the transmission distance. Although the transmission distance of SQKD still depends on the forward channel, the longest SQKD transmission distance reaches 134 km with the addition of one decoy states. It is 21 km shorter than the farthest transmission of QKD when $\mu = 0.68$ and $\nu = 0.08$.

3.2.2 Adding decoy states to Bob

If Bob also chooses to add one decoy state, Alice sends two pulses with different photon numbers, and Bob also resends two pulses with different photon numbers. Thus, the forward channel has a one decoy state, and the backward channel has a three decoy states.

If Bob resends a signal state without the decoy state, Alice sends two pulses of different photon numbers, and Bob sends only one pulse with a photon number. Thus, the forward channel has one decoy state, and the backward channel has two decoy states.

The backward channel always has more decoy states than the forward channel. Moreover, the longest transmission distance of the forward channel L_f must be less than that of the backward channel L_b. If a decoy state is also added to the backward channel, the vacuum state can be added to obtain a tighter Y_0 and increase the transmission distance of the backward channel; however, the final distance is the shortest result because $L_f = L_b$ (same physical channel). Therefore, adding a decoy state to the backward channel is unnecessary and makes the experiment more complicated.

3.2.3 Comparing different decoy states

We can add weak+vacuum decoy states to Alice. We set $\mu_1 = 0.36$; $\nu_1 = 0.08$; and $\mu_3 = 0.68$. Although this configuration is not the optimal setting for two decoy states, we can conclude by a simple comparison with one decoy state. Then, we add $\nu_2 = 0$ to Alice. In the two decoy states, estimation of Y_0 is:

$$Y_{0_{two}} = \frac{\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1}}{\nu_1 - \nu_2}. \tag{25}$$

The estimation of Y_1 is:

$$Y_{1_{two}} = \frac{\mu}{\mu\nu_1 - \mu\nu_2 - {\nu_1}^2 + {\nu_2}^2}\left[Q_{\nu_1}e^{\nu_1} - Q_{\nu_2}e^{\nu_2} - \frac{{\nu_1}^2 - {\nu_2}^2}{\mu^2}\left(Q_\mu e^\mu - Y_0\right)\right]. \tag{26}$$

And the estimation of e_1 is:

$$e_{1_{two}} = \frac{E_{\nu_1}Q_{\nu_1}e^{\nu_1} - E_{\nu_2}Q_{\nu_2}e^{\nu_2}}{Y_1(\nu_1 - \nu_2)}. \tag{27}$$

In Fig. 5(b), we can observe that the transmission distance of two decoy states is longer than that of one decoy state. The longest transmission distance using the SQKD secure bit rate can reach 149 km. The maximal distance of forward channel is 152 km. The maximal distance of backward channel is 155 km. Therefore, the SQKD transmission distance is 149 km. This significantly lengthens the transmission distance of the forward channel, but in general, the SQKD transmission distance increases 15 km.

4 Results and discussion

By modeling an SQKD channel and adding decoy states, an SQKD system was able to detect a PNS attack. We estimated the longest transmission distance and secure bit rate using the GLLP theory and decoy states under an asymptotic condition. In this study, we assumed that the two channels were independent and that Eve's attacks were also independent. Owing to the correlation between Alice and $Alice'$, it is important to determine the physical model of the channels if they are not independent. Eve will definitely attack the correlation between the two channels; therefore, we will address this issue in future work. Optimizing the strength of different kinds of decoy states to maximize SQKD performance is also our subsequent research work. Moreover, we will also consider the finite-key in practical application.

5 Conclusion

We determine SQKD can't resist PNS attacks. We first model the SQKD channel model and get the secure bit rate formula of SQKD to evaluate the experimental safety of SQKD. Moreover, we add decoy states to SQKD to estimated the longest transmission distance. it is important that SQKD can also use decoy state methods to make experiments more secure using essentially the same hardware.

Acknowledgements

The authors thank the Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials and Bluedon Information Security Technology Co., Ltd.

Funding

National Science Foundation of China (62071186, 61771205); National Science Foundation of Guangdong Province (2015A030313388); Science and Technology Planning Projects of Guangdong Province (2015B010128012, 2017KZ010101); Guangdong Provincial Key Laboratory (grant no. 2020B1212060066).

Availability of data and materials

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Declarations

Competing interests

The authors declare no competing interests.

Author contributions

All authors read and approved the final manuscript.

Author details

[1]Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou 510006, China. [2]Guangdong Provincial Key Laboratory of Nanophotonic Functional Materials and Devices, School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou 510006, China. [3]Department of Optoelectronic Engineering, Jinan University, Guangzhou 510632, China.

Received: 31 May 2022 Accepted: 18 May 2023 Published online: 31 May 2023

References

1. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560:7–11.
2. Muller A, Herzog T, Huttner B, Tittel W, Zbinden H, Gisin N. "Plug and play" systems for quantum cryptography. Appl Phys Lett. 1997;70(7):793–5. https://doi.org/10.1063/1.118224.
3. Wang J, Qin X, Jiang Y, Wang X, Chen L, Zhao F, Wei Z, Zhang Z. Experimental demonstration of polarization encoding quantum key distribution system based on intrinsically stable polarization-modulated units. Opt Express. 2016;24(8):8302–9. https://doi.org/10.1364/OE.24.008302.
4. Mo X-F, Zhu B, Han Z-F, Gui Y-Z, Guo G-C. Faraday–Michelson system for quantum cryptography. Opt Lett. 2005;30(19):2632–4. https://doi.org/10.1364/OL.30.002632.
5. Zhang C-H, Zhou X-Y, Ding H-J, Zhang C-M, Guo G-C, Wang Q. Proof-of-principle demonstration of passive decoy-state quantum digital signatures over 200 km. Phys Rev Appl. 2018;10:034033. https://doi.org/10.1103/PhysRevApplied.10.034033.
6. Wang J, Qin X, Jiang Y, Wang X, Chen L, Zhao F, Wei Z, Zhang Z. Experimental demonstration of polarization encoding quantum key distribution system based on intrinsically stable polarization-modulated units. Opt Express. 2016;24(8):8302–9. https://doi.org/10.1364/OE.24.008302.
7. Zhou X-Y, Zhang C-H, Zhang C-M, Wang Q. Asymmetric sending or not sending twin-field quantum key distribution in practice. Phys Rev A. 2019;99:062316. https://doi.org/10.1103/PhysRevA.99.062316.
8. Liu J-Y, Ding H-J, Zhang C-M, Xie S-P, Wang Q. Practical phase-modulation stabilization in quantum key distribution via machine learning. Phys Rev Appl. 2019;12:014059. https://doi.org/10.1103/PhysRevApplied.12.014059.
9. Chen Y-P, Liu J-Y, Sun M-S, Zhou X-X, Zhang C-H, Li J, Wang Q. Experimental measurement-device-independent quantum key distribution with the double-scanning method. Opt Lett. 2021;46(15):3729–32. https://doi.org/10.1364/OL.431061.
10. Yuan Y-P, Du C, Shen Q-Q, Wang J-D, Yu Y-F, Wei Z-J, Chen Z-X, Zhang Z-M. Proof-of-principle demonstration of measurement-device-independent quantum key distribution based on intrinsically stable polarization-modulated units. Opt Express. 2020;28(8):10772–82. https://doi.org/10.1364/OE.387968.
11. Lutkenhaus N. Security of quantum cryptography with realistic sources. Acta Phys Slovaca. 1999;**49**.
12. 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. https://doi.org/10.1103/PhysRevLett.95.080501.
13. Hwang WY, Ahn DD, Hwang SW. Eavesdropper's optimal information in variations of Bennett–Brassard 1984 quantum key distribution in the coherent attacks. Phys Lett A. 2001;279(3):133–8. https://doi.org/10.1016/S0375-9601(00)00825-2.
14. Dušek M, Haderka O, Hendrych M. Generalized beam-splitting attack in quantum cryptography with dim coherent states. Opt Commun. 1999;169(1):103–8. https://doi.org/10.1016/S0030-4018(99)00419-8.
15. Brassard G, Lütkenhaus N, Mor T, Sanders BC. Limitations on practical quantum cryptography. Phys Rev Lett. 2000;85:1330–3. https://doi.org/10.1103/PhysRevLett.85.1330.
16. Bennett CH. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett. 1992;68:3121–4. https://doi.org/10.1103/PhysRevLett.68.3121.
17. Huttner B, Imoto N, Gisin N, Mor T. Quantum cryptography with coherent states. Phys Rev A. 1995;51:1863–9. https://doi.org/10.1103/PhysRevA.51.1863.
18. Hwang W-Y. Quantum key distribution with high loss: toward global secure communication. Phys Rev Lett. 2003;91:057901. https://doi.org/10.1103/PhysRevLett.91.057901.
19. Lo H-K, Ma X, Chen K. Decoy state quantum key distribution. Phys Rev Lett. 2005;94:230504. https://doi.org/10.1103/PhysRevLett.94.230504.
20. Wang X-B. Beating the photon-number-splitting attack in practical quantum cryptography. Phys Rev Lett. 2005;94:230503. https://doi.org/10.1103/PhysRevLett.94.230503.
21. Ma X, Qi B, Zhao Y, Lo H-K. Practical decoy state for quantum key distribution. Phys Rev A. 2005;72:012326. https://doi.org/10.1103/PhysRevA.72.012326.
22. Wang Q, Wang X-B, Guo G-C. Practical decoy-state method in quantum key distribution with a heralded single-photon source. Phys Rev A. 2007;75:012312. https://doi.org/10.1103/PhysRevA.75.012312.
23. Ma X, Fung C-HF, 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. https://doi.org/10.1103/PhysRevA.74.032330.
24. Scarani V, Acín A, Ribordy G, Gisin N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys Rev Lett. 2004;92:057901. https://doi.org/10.1103/PhysRevLett.92.057901.
25. Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob. Phys Rev Lett. 2007;99:140501. https://doi.org/10.1103/PhysRevLett.99.140501.
26. Boyer M, Gelles R, Kenigsberg D, Mor T. Semiquantum key distribution. Phys Rev A. 2009;79:032341. https://doi.org/10.1103/PhysRevA.79.032341.

27. Zou X, Qiu D, Li L, Wu L, Li L. Semiquantum-key distribution using less than four quantum states. Phys Rev A. 2009;79:052312. https://doi.org/10.1103/PhysRevA.79.052312.
28. Boyer M, Katz M, Liss R, Mor T. Experimentally feasible protocol for semiquantum key distribution. Phys Rev A. 2017;96:062335. https://doi.org/10.1103/PhysRevA.96.062335.
29. Amer O, Krawec WO. Semiquantum key distribution with high quantum noise tolerance. Phys Rev A. 2019;100:022319. https://doi.org/10.1103/PhysRevA.100.022319.
30. Zhang W, Qiu D, Mateus P. Single-state semi-quantum key distribution protocol and its security proof. Int J Quantum Inf. 2020;18(04):2050013. https://doi.org/10.1142/S0219749920500136.
31. Krawec WO, Liss R, Mor T. Security proof against collective attacks for an experimentally feasible semi-quantum key distribution protocol. 2020. arXiv preprint. arXiv:2012.02127.
32. Han S, Huang Y, Mi S, Qin X, Wang J, Yu Y, Wei Z, Zhang Z. Proof-of-principle demonstration of semi-quantum key distribution based on the mirror protocol. EPJ Quantum Technol. 2021;8(1):28. https://doi.org/10.1140/epjqt/s40507-021-00117-8.
33. Gottesman D, Lo H-K, Lutkenhaus N, Preskill J. Security of quantum key distribution with imperfect devices. In: International symposium onInformation theory, 2004. Proceedings. 2004. p. 136. https://doi.org/10.1109/ISIT.2004.1365172.
34. Lütkenhaus N, Jahma M. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. New J Phys. 2002;4(1):44.
35. Csiszár I, Korner J. Broadcast channels with confidential messages. IEEE Trans Inf Theory. 1978;24(3):339–48.
36. Shor PW, Preskill J. Simple proof of security of the bb84 quantum key distribution protocol. Phys Rev Lett. 2000;85:441–4. https://doi.org/10.1103/PhysRevLett.85.441.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.