New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG IOP Institute of Physics

# Quantum key distribution with triggering parametric down-conversion sources

To cite this article: Xiongfeng Ma and Hoi-Kwong Lo 2008 *New J. Phys.* **10** 073018

New Journal of Physics
The open-access journal for physics

# Quantum key distribution with triggering parametric down-conversion sources

**Xiongfeng Ma**[1] **and Hoi-Kwong Lo**[1]
Center for Quantum Information and Quantum Control,
Department of Electrical Computer Engineering and Department of Physics,
University of Toronto, Toronto, ON M5S 1A7, Canada
E-mail: xima@physics.utoronto.ca and hklo@comm.utoronto.ca

*New Journal of Physics* **10** (2008) 073018 (22pp)
Received 17 March 2008
Published 9 July 2008
Online at http://www.njp.org/
doi:10.1088/1367-2630/10/7/073018

**Abstract.** Parametric down-conversion (PDC) sources can be used as triggered single photon sources in quantum key distribution (QKD). Recently, there have been several practical proposals of the decoy state QKD with triggering PDC sources. In this paper, we generalize the passive decoy state idea, originally proposed by Mauerer and Silberhorn. The generalized passive decoy state idea can be applied to cases where either threshold detectors or photon-number-resolving detectors are used. The decoy state protocol proposed by Adachi, Yamamoto, Koashi and Imoto (AYKI) can be treated as a special case of the generalized passive decoy state method. By simulating a recent PDC experiment, we compare various practical decoy state protocols with the infinite decoy state protocol and also compare the cases using threshold detectors and photon-number-resolving detectors. Our simulation result shows that with the AYKI protocol, one can achieve a key generation rate that is close to the theoretical limit of an infinite decoy state protocol. Furthermore, our simulation result shows that a photon-number-resolving detector appears to be not very useful for improving QKD performance in this case. Although our analysis is focused on QKD with PDC sources, we emphasize that it can also be applied to QKD setups with other triggered single photon sources.

[1] Correspondence may be addressed to either of the authors.

## Contents

## 1. Introduction

Quantum key distribution (QKD) [1, 2] allows two legitimate parties, Alice and Bob, to create a random secret key even when the channel is accessible to an eavesdropper, Eve. The security of QKD is built on the fundamental laws of physics in contrast to existing classical public key encryption schemes that are based on unproven computational assumptions. Proving the security of QKD is a tough problem. Fortunately, this problem has been solved in the last decade, see for example [3]–[6]. Many security proofs are based on the assumption of idealized QKD system components, such as a perfect single photon source and well-characterized detectors. In practice, inevitable device imperfections may compromise the security unless these imperfections are well investigated. Meanwhile, the security of QKD with realistic devices has been proven, see [7]–[12] for example.

Bennett and Brassard proposed the best-known protocol—BB84 [1]. In the original proposal of the BB84 protocol, a single photon source is used. Unfortunately, single photon sources are still not commercially available with current technology. Alternatively, a weak coherent state is widely used as a photon source. We call this implementation *coherent state QKD*. Many coherent state QKD experiments have been done since the first QKD experiment [13].

Coherent state QKD suffers from photon-number splitting (PNS) attacks [9, 14, 15]. Nevertheless, it has been proven unconditionally secure by Inamori, Lütkenhaus and Mayers [10]. This work was improved by Gottesman, Lo, Lütkenhaus, and Preskill (GLLP) [12], though the performance in terms of the achievable secure distance and the key rate is limited.

Decoy state method [16] has been proposed for improving the performance of coherent state QKD. The security of QKD with decoy states has been proven [17]–[19]. Simulation results show us that the coherent state QKD with decoy states is able to operate as good as QKD with perfect single photon sources in the sense that the key generation rates given by both setups depend linearly on the channel transmittance [19]. Later, some practical decoy state protocols with only one or two decoy states were proposed [20], see also [21]–[23]. Experimental demonstrations for the decoy state method have been done recently [24]–[29].

The motivation of decoy states is to estimate the channel properties (e.g. transmittance and error probability) better. To do that, Alice uses extra states with different light intensities during key transmission. Then Alice and Bob can consider detection statistics from signal and decoy states separately, from which they can estimate the channel transmittance and error probability better. We call the situation when Alice actively prepares decoy states the *active decoy state* method to differentiate from the *passive decoy state* method where Alice chooses decoy and signal states by passive measurements. Details of the passive decoy state method can be found in section 4. We note that in the coherent state QKD, one can only use the active decoy state method.

Other than the decoy state method, we remark that there are other approaches for enhancing the performance of the coherent state QKD, such as QKD with strong reference pulses [30, 31] and differential-phase-shift QKD [32].

Besides a coherent state source, a parametric down-conversion (PDC) source can also be used for QKD. There are two ways of using a PDC source for QKD. The first is to use it as a triggered (heralded) single photon source. Alice detects one of the two beams, the idle beam, from a PDC source as a trigger[2] and actively encodes her qubit information into another beam, the signal beam. We call this implementation *triggering PDC QKD*. The second way is to use it as an entangled photon source for entanglement-based QKD protocols [2, 33]. We call this implementation *entanglement PDC QKD*. See, for example [34] and references cited therein.

The triggering PDC QKD, similar to the coherent state QKD, suffers from PNS attacks. By applying the GLLP security proof, one can find that the optimal average photon number $\mu$ is in the same order as the overall transmittance $\eta$. Then the key generation rate will be in the order of $\eta^2$. For a rigorous derivation, one can refer to the appendix. Thus, the performance of the triggering PDC QKD is very limited.

Since the decoy state idea can substantially enhance the performance of the coherent state QKD, a natural question will be: 'can the decoy state idea be applied to the triggering PDC QKD?' The answer is *yes*. One can apply the infinite decoy state idea [19] to the triggering PDC QKD. Not surprisingly, with decoy states, the key generation rate can be $O(\eta)$, which is the same as the order achieved by a perfect single-photon source. Therefore, we expect the decoy state QKD to become a standard technique not only in the coherent state QKD, but also in the triggering PDC QKD. The infinite decoy state protocol requires an infinite number of decoy states to be used, which is not practical. A few practical decoy proposals for triggering PDC QKD requiring a finite number of decoy states have been proposed [35]–[38].

[2] See section 2 for the definition of a trigger.

We are interested in comparing various protocols for the triggering PDC QKD. Among the practical decoy state protocols, we find that the one proposed by Adachi, Yamamoto, Koashi and Imoto (AYKI) [36] is simple to implement. The AYKI protocol is conceptually similar to the one-decoy-state scheme [20]. In the AYKI protocol, Alice and Bob only need to consider the statistics of triggered and non-triggered detection events[3] separately, instead of preparing new signals for decoy states. We emphasize that the AYKI protocol is easy to implement since there is no need for a hardware change.

Other decoy state proposals for the triggering PDC QKD require hardware modifications. For example, the one proposed by Mauerer and Silberhorn [35] requires photon-number-resolving detectors, and the one proposed by Wang, Wang and Guo [37] requires Alice to pump the laser source at various intensities.

We generalize the passive decoy state idea proposed by Mauerer and Silberhorn [35]. The main idea is that Bob can group his detection events according to the public announcement of Alice's detection events. For example, when Alice uses a threshold detector, Bob can group his detection results according to whether Alice gets a detection or not. The generalized passive decoy state idea can be applied to both cases of using threshold detectors and photon-number-resolving detectors. The AYKI protocol can be treated as a special case of the generalized passive decoy state protocol.

By simulating a recent PDC experiment [39], we compare one case with a perfect photon-number-resolving detector and four cases with threshold detectors: no decoy, infinite decoy, weak decoy and AYKI. Our simulation result shows that in a large parameter regime, the performance of the AYKI protocol is close to that of the infinite decoy state protocol and thus there is not much room left for improvement after the AYKI protocol has been implemented. Also, the QKD performance of the case with the infinite decoy state protocol using threshold detectors is close to the case using a perfect photon-number-resolving detector. Thus, a photon-number-resolving detector appears to be not very useful for the triggering PDC QKD.

We emphasize that one advantage of passive decoy state method is that by passively choosing decoy and signal states, the possibility that Eve can distinguish decoy and signal states is reduced. On the other hand, in active (regular) decoy state experiments, it is more difficult to verify the assumption that Eve cannot distinguish decoy and signal states.

We note that the passive decoy state idea can be combined with the active decoy state idea. In [38], the authors gave a special case of combining passive and active decoy state ideas. Note that for the coherent state QKD, one can only use active decoy state methods.

Although our analysis focuses on the QKD with PDC sources, we emphasize that it can also be applied to QKD setups with other triggered single photon sources.

In section 2, we will review the experimental setup of the triggering PDC QKD. In section 3, we will give a model for the triggering PDC QKD. In section 4, we will study various post-processing schemes for the triggering PDC QKD. In section 5, we will compare various schemes of the triggering PDC QKD: non-decoy + threshold detectors, infinite decoy + threshold detectors, AYKI and the case with a perfect photon-number-resolving detector, by simulating a real PDC experiment. In the appendix, we consider the optimal PDC source intensities for the triggering PDC QKD.

[3] In a non-triggered detection event, Bob gets a detection but Alice doesn't get a trigger.

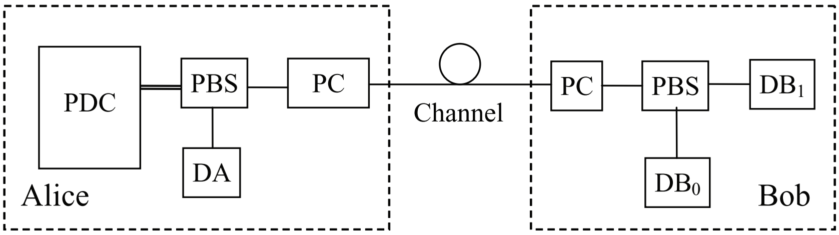

**Figure 1.** A schematic diagram for the triggering PDC QKD. Alice collects photon pairs emitted from a PDC source and uses a polarized beam splitter (PBS) to separate two polarization modes. She detects one of the two modes with her detector (DA) as a trigger, modulates the polarization of the other mode by a polarization controller (PC) and sends it to Bob. On Bob's side, he chooses his basis using a PC and performs a measurement using his detectors (DB$_0$ and DB$_1$).

## 2. Experimental setup

In the triggering PDC QKD, a PDC source is used as a triggered single photon source[4]. The schematic diagram is shown in figure 1.

As shown in figure 1, a PDC source generates two modes of photons, which can be separated by a PBS. One mode goes to Alice's own detector (DA in figure 1) as the triggering signal and the other mode is used as a triggered single photon state for the QKD. When Alice's detector (DA) clicks, we call it a *trigger*. We divide the detection events on Bob's side into two groups depending on whether Alice gets a trigger or not: triggering detection events and non-triggering detection events.

Note that Alice can use either a threshold detector or a photon-number-resolving detector (DA in figure 1). She only needs to know the number of photons in the trigger mode. So only one detector is sufficient on Alice's side. Due to the high channel losses, without Eve's interference, Bob is highly likely to receive a vacuum or single photon state. Thus it is sufficient for Bob to use threshold detectors. Threshold single photon detectors can only tell whether there is a click or not, but not the photon numbers. Here we assume Alice encodes qubit information in photon polarizations. Hence, Bob needs to identify polarizations of incoming photons.

In real experiments, there are two types of PDC sources. In the triggering PDC QKD, both of these two types can be used. Here we assume Alice uses a type-II PDC source. The Hamiltonian of the type-II PDC process in the triggering setup shown in figure 1 can be written as [40]

$$H = \mathrm{i}\chi a^\dagger b^\dagger + \mathrm{h.c.}, \tag{1}$$

where h.c. means Hermitian conjugate and $\chi$ is a coupling constant which depends on the crystal nonlinearity and the amplitude of the pump beam. The operators $a^\dagger$, $b^\dagger$ and $a$, $b$ are the creation and annihilation operators of two modes with different polarizations.

The state coming from a PDC source, with a Hamiltonian of equation (1), can be written as [40]

$$|\Psi\rangle = (\cosh\chi)^{-1}\sum_{n=0}^{\infty}(\tanh\chi)^n|n, n\rangle. \tag{2}$$

[4] Sometimes it is called a heralded single photon source.

Here we assume the state is single-mode. The expected photon pair number is given by $\mu = \sinh^2\chi$. The probability to get an $n$-photon pair is

$$P(n) = \frac{\mu^n}{(1+\mu)^{n+1}}. \tag{3}$$

Here, we assume that the PDC source always sends out photon pairs. That is, the photon number of mode $a$ and $b$ are always the same.

There is a nonzero probability for the PDC source to emit more than one photon pair in one pulse. Thus, Alice may send out multi-photon states after she encodes basis and key information using her PC. This is the reason why the triggering PDC QKD suffers from PNS attacks.

Let us compare the experimental setups of the triggering PDC QKD and entanglement PDC QKD implementations. For the entanglement PDC QKD setup, one can refer to [34], [41]–[43]. In the triggering PDC QKD, Alice actively encodes the key information, while in the entanglement PDC QKD Alice passively encodes the key by measuring the polarization of one of the two beams from the PDC source. The advantage of the triggering PDC QKD here is that it does not rely on the polarization correlations between two beams of the PDC source. It only requires photon-pair generation of the source, which means the entanglement between photon pairs is not important for the triggering PDC QKD. However, in the entanglement PDC QKD implementation, the entanglement between two beams needs to be generated. We notice that the generation and maintenance of the entanglement in real experiments is a highly nontrivial task [44]. For example, one needs to eliminate the possibilities of distinguishing photons during the pair generation procedure.

## 3. Model

Lütkenhaus has already studied the model of the triggering PDC QKD [8] with threshold detectors. His model is similar to the one of the coherent state QKD, except for a different photon number distribution. For the model of the coherent state QKD, one can refer to [8, 20].

### *3.1. Photon-number channel model*

Here, we will use the photon-number channel model [19]: Alice and Bob have infinite numbers of channels. For channel $i$, Alice uses $i$-photon states (Fock states) for carrying the qubit information, with $i = 0, 1, 2, \ldots$. The $i$th channel corresponds to the case when Alice's photon source emits an $i$-photon state. Thus, the probability of Alice using the $i$th channel is determined by the photon source. For example, in the coherent state QKD, the probability of Alice using the different channels follows a Poisson distribution.

We define the yield $Y_i$ to be the probability of Bob getting a detection event conditioned on Alice using the $i$th channel. As discussed in section 2, we assume that Bob uses threshold detectors. The yield is given by

$$Y_i = 1 - (1 - Y_{0\mathrm{B}})(1-\eta)^i, \tag{4}$$

where $Y_{0\mathrm{B}}$ is the background count rate of Bob's detection system, and $\eta$ is the overall detection probability for Bob, which takes into account the channel transmission efficiency, the coupling efficiency, the detector efficiency and the other losses in Bob's box.

The error rate when Alice uses the $i$th channel is given by

$$e_i Y_i = e_{\mathrm{d}} Y_i + (e_0 - e_{\mathrm{d}}) Y_{0\mathrm{B}}, \tag{5}$$

where $e_0 = 1/2$ is the error rate of background counts, $e_{\mathrm{d}}$ the intrinsic detector error rate on Bob's side (e.g. due to misalignment)[5] and $Y_i$ is given by equation (4). Here, we neglect the case where both background counts and true signal click, since $\eta$ and $Y_{0\mathrm{B}}$ are small. We remark that equations (4) and (5) are true for both triggered and non-triggered detections.

### 3.2. On Alice's side

In the triggering PDC QKD, Alice may use either a threshold detector or a photon-number-resolving detector. Define an *N-photon-resolving* detector to be a detector that can tell 0, 1, ... , $N$ photons in an incoming signal. For a threshold detector, we have $N = 1$, which can only tell whether there are photons present or not. Given an incoming $i$-photon state, the probability of Alice's detector indicating a $j$-photon state is $\eta_{j|i}$, with $\sum_{j=0}^{j=N} \eta_{j|i} = 1$ for all $i = 0, 1, \ldots$. In general, $\eta_{j|i}$s are real numbers in [0,1]. We define a $j$-photon trigger for the case that Alice's detector indicates a $j$-photon state.

For a triggered PDC photon source, as given in equation (2), the probability of Alice's detector indicating a $j$-photon detection is

$$P_{\mathrm{A}j} = \sum_{i=0}^{\infty} \frac{\mu^i}{(1+\mu)^{i+1}} \eta_{j|i}. \tag{6}$$

With the assumption that the PDC source always emits photon pairs, the probability (gain) of Alice getting a $j$-photon detection and Bob getting a detection is

$$Q_{\mu,j} = \sum_{i=0}^{\infty} Q_{i,j} = \sum_{i=0}^{\infty} \frac{\mu^i}{(1+\mu)^{i+1}} \eta_{j|i} Y_i, \tag{7}$$

where the yield $Y_i$ is given in equation (4). The quantum bit error rate (QBER) conditioned on Alice's $j$-photon detection, similar to equation (7), is given by

$$E_{\mu,j} Q_{\mu,j} = \sum_{i=0}^{\infty} Q_{i,j} e_i = \sum_{i=0}^{\infty} \frac{\mu^i}{(1+\mu)^{i+1}} \eta_{j|i} Y_i e_i, \tag{8}$$

where the error rate $e_i$ is given in equation (5).

One observation is that in the triggering PDC QKD setup, shown in figure 1, the quantities $Y_i$ and $e_i$ are independent of Alice's measurement outcome $j$. This is based on the single-mode PDC source assumption described in equation (1) in section 2.

### 3.3. Threshold detector

Here, we will discuss a special case that Alice uses a threshold detector. That is,

$$\begin{aligned} &\eta_{0|i} = (1 - Y_{0A})(1 - \eta_A)^i \simeq (1 - \eta_A)^i, \\ &\eta_{1|i} = 1 - \eta_{0|i}, \qquad \eta_{j|i} = 0, \qquad \forall j \geqslant 2, \end{aligned} \tag{9}$$

where $Y_{0\mathrm{A}}$ and $\eta_{\mathrm{A}}$ are the background count rate and the detector efficiency on Alice's side. The approximation is due to the fact that normally we have $\eta_A \gg Y_{0A}$. That is, we neglect the background contributions on Alice's side.

[5] For a real detection system, the intrinsic detector error rate can be calculated by $e_{\mathrm{d}} = (1 - V)/2$, where $V$ is the visibility of the detection system.

According to equations (7) and (8), without Eve's interference, the gains and QBERs of triggered ($j = 1$) and non-triggered ($j = 0$) detections are given by

$$\begin{aligned}
Q_{\mu,0} &= \frac{1}{1+\eta_A\mu} - \frac{1-Y_{0B}}{1+(\eta_A+\eta-\eta_A\eta)\mu},\\
Q_{\mu,1} &= 1 - \frac{1}{1+\eta_A\mu} - \frac{1-Y_{0B}}{1+\eta\mu} + \frac{1-Y_{0B}}{1+(\eta_A+\eta-\eta_A\eta)\mu},\\
E_{\mu,0}Q_{\mu,0} &= e_d Q_{\mu,0} + \frac{(e_0-e_d)Y_{0B}}{1+\eta_A\mu},\\
E_{\mu,1}Q_{\mu,1} &= e_d Q_{\mu,1} + \frac{(e_0-e_d)\eta_A\mu Y_{0B}}{1+\eta_A\mu}.
\end{aligned} \tag{10}$$

Without Eve's interference, the gains and error rates of the single photon state in two detections are given by

$$\begin{aligned}
Q_{1,0} &= \frac{\mu(1-\eta_A)}{(1+\mu)^2}Y_1,\\
Q_{1,1} &= \frac{\mu\eta_A}{(1+\mu)^2}Y_1,\\
e_1Y_1 &= e_dY_1 + (e_0-e_d)Y_{0B},
\end{aligned} \tag{11}$$

where $Y_1$ and $e_1$ are given in equations (4) and (5), respectively.

### 3.4. *Perfect photon-number-resolving detector*

Here, we will discuss the case in which Alice uses a perfect photon-number-resolving detector, which can faithfully tell the number of photons in the incoming signal. That is, $\eta_{j|i} = \delta_{ij}$. Thus the gains and QBERs are given by, from equations (7) and (8),

$$\begin{aligned}
Q_{\mu,i} &= Q_{i,i} = \frac{\mu^i}{(1+\mu)^{i+1}}Y_i,\\
E_{\mu,i}Q_{\mu,i} &= e_iQ_{i,i} = \frac{\mu^i}{(1+\mu)^{i+1}}e_iY_i,
\end{aligned} \tag{12}$$

from which one can directly infer the gains and error rates of the $i$-photon state, $Q_{i,j} = Q_{i,i}\delta_{i,j}$.

## 4. Post-processing

In this section, we will first review the GLLP security analysis, based on which we figure out the parameters needed to be estimated in the post-processing. Then, we present different ways of estimating these parameters.

1. In section 4.2, we consider the case of non-decoy states with threshold detectors.
2. In section 4.3, we consider the case of infinite decoy states with threshold detectors.
3. In section 4.4, we consider the case of weak decoy states with threshold detectors, which is essentially the work done by Wang, Wang and Guo [37].
4. In section 4.5, we generalize the idea of a passive decoy state proposed by Mauerer and Silberhorn [35].

5. In section 4.6, we consider the post-processing protocol proposed by AYKI [36], which turns out to be a special case of the generalized passive decoy state method.
6. In section 4.7, we consider another special case of the passive decoy state protocol: Alice has a perfect photon-number-resolving detector that can tell the exact photon number of the incoming pulse.

### *4.1. GLLP security analysis*

In the following discussion, we will focus on the BB84 protocol [1]. Due to PNS attacks [9, 14, 15], only vacuum states and single photon states are secure for BB84 protocol, which may not be true for other protocols, such as SARG04 [45, 46].

Similar to the coherent state QKD, we can apply GLLP [12] security analysis to the triggering PDC QKD. Note that in the GLLP security analysis, the squash model is assumed. With the squash model, one can assume that Bob always receives a vacuum or qubit [47]–[49].

The post-processing of GLLP is performed as follows. First, Alice and Bob perform error correction, after which they will share an identical key. Then, they perform privacy amplification on different types of qubits separately. Since here we assume only vacuum states and single photon states are secure for the BB84 protocol, the key generation rate is given by [19, 47, 50]

$$R \geqslant q\{-f(E_\mu)Q_\mu H_2(E_\mu) + Q_1[1 - H_2(e_1)] + Q_0\}, \tag{13}$$

where $q$ is the basis reconciliation factor (1/2 for the BB84 protocol due to the fact that half of the time Alice and Bob disagree with the bases, and if one uses the efficient BB84 protocol [51], $q \approx 1$), the subscript $\mu$ denotes the expected photon pair number, $Q_\mu$ and $E_\mu$ are the overall gain and QBER, $Q_1$ and $e_1$ are the gain and error rate of single photon states, $Q_0$ is the gain of vacuum states, $f(x)$ is the error correction efficiency (see, for example, [52]) as a function of the error rate (normally $f(x) \geqslant 1$ with the Shannon limit $f(x) = 1$) and $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function.

All the classical data measured can be grouped according to Alice's detection events, $j = 0, 1, \ldots, N$. Then we can apply the GLLP idea [12, 53] to each group. The final key generation rate will be given by summing over contributions from all the groups,

$$R = \sum_{j=0}^{N} R_j. \tag{14}$$

In each case $j$, one can apply equation (13),

$$R_j \geqslant q\Big\{-f(E_{\mu,j})Q_{\mu,j}H_2(E_{\mu,j}) + Q_{1,j}[1 - H_2(e_1)] + Q_{0,j}\Big\}, \tag{15}$$

where $Q_{0,j}$ and $Q_{1,j}$ are the first and second terms in the right-hand side of equation (7). Here the error rate of single photon state $e_1$ is independent of $j$, see the observation at the end of section 3.2. We note that the key generation rate from all $j$-photon trigger detections should be non-negative. If any of them contributes a negative key generation rate, we should assign it 0. In this case, Alice and Bob can just discard those types of detections. Based on this observation, we can further simplify equation (14). Given that Alice detects more than one photon, the probability of emitting a single photon state in Bob's arm is small[6]. As we mentioned at the beginning of this section, only vacuum and single photon state can contribute positively to the final key rate. Thus we can focus on the case $j = 0, 1$.

$$R = R_0 + R_1, \tag{16}$$

where $R_0$ and $R_1$ are given in equation (15). Again, both $R_0$ and $R_1$ should be non-negative, otherwise should be assigned 0.

In equation (15), the gain $Q_{\mu,j}$ and the QBER $E_{\mu,j}$, given in equations (7) and (8), can be measured or tested from QKD experiments directly. In this section, we will discuss various ways of estimating $Q_{0,j}$, $Q_{1,j}$, and $e_1$. We assume that the PDC photon source and detector characteristics are fixed and known to Alice. That is, $\mu$, the photon number distribution in equation (3) and $\eta_A$ are fixed and known.

### 4.2. Non-decoy states with threshold detectors

Here we assume that Alice uses a threshold detector. Thus, Alice only has two measurement outcomes, $j = 0, 1$. One simple way of estimating $Q_{0,j}$, $Q_{1,j}$, and $e_1$ is by assuming that all losses and errors come from the single photon states. This is because Eve can in principle perform PNS attacks on the multi-photon states. The gain and error rates of the single photon states in triggered ($j = 1$) and non-triggered ($j = 0$) detections can be bounded by

$$\begin{aligned}
Q_{1,0} &\geqslant Q_{\mu,0} - \textstyle\sum_{i=2}^{\infty} \frac{\mu^i}{(1+\mu)^{i+1}} \eta_{0|i} \\
&= Q_{\mu,0} - \frac{(1-\eta_A)^2\mu^2}{(1+\eta_A\mu)(1+\mu)^2}, \\
Q_{1,1} &\geqslant Q_{\mu,1} - \frac{\eta_A(2-\eta_A+\mu)\mu^2}{(1+\eta_A\mu)(1+\mu)^2}, \\
e_{1,0} &\geqslant \frac{E_{\mu,0}Q_{\mu,0}}{Q_{1,0}}, \\
e_{1,1} &\geqslant \frac{E_{\mu,1}Q_{\mu,1}}{Q_{1,1}},
\end{aligned} \tag{17}$$

where $\eta_A$ is the efficiency of Alice's detector. The gain $Q_\mu$ and the QBER $E_\mu$, given in equations (7) and (8), can be measured or tested from QKD experiments directly. In the following simulations, we will use equation (10). Since we assume all errors come from the single photon states, one should take the lower bound of the vacuum contribution to be $Q_{0,j} = 0$.

### 4.3. Infinite active decoy state with threshold detectors

To do privacy amplification, Alice and Bob need to bound $Q_{0,j}$, $Q_{1,j}$, and $e_1$ for equation (15). From equation (7), we know that to bound $Q_{1,j}$, Alice and Bob need to estimate $Y_1$.

[6] In section 2, we assume that Alice's PDC source always sends out photon pairs. Given that Alice detects more than one photon on the triggering arm, a single photon state presents on the other arm only when there is a dark count in Alice's detector. Normally, we can assume that the detector efficiency is much higher than the dark count probability on Alice's side. Thus, we neglect the probability of a single photon state with a multi-photon trigger.

The decoy state method provides a good way of estimating $Y_1$ and $e_1$ [16, 19]. The essential idea is that instead of considering each linear equation of $Y_1$ and $e_1$ in the form of equations (7) and (8) separately, Alice and Bob consider all the linear equations simultaneously.

Let us imagine that Alice and Bob obtain an infinite number of linear equations in the form of equations (7) and (8), e.g. they use an infinite number of intensities $\mu$. In principle, Alice and Bob can solve the equations to get $Y_1$ and $e_1$ accurately. Mathematically, the problem is solvable. The intuition is that the contributions from higher order terms of $Y_i$ and $e_i$ decrease exponentially in equations (7) and (8). For the case of coherent state QKD, one or two decoy states have been proved to be sufficient [20]. Shortly, we will see that one decoy state is sufficient for the triggering PDC QKD.

We remark that the key underlying assumption of the decoy state method is [19]

$$Y_i(\text{decoy}) = Y_i(\text{signal}), \qquad e_i(\text{decoy}) = e_i(\text{signal}). \tag{18}$$

In other words, Eve sets the same values of $Y_i$ and $e_i$ for decoy and signal states. This can be guaranteed by the assumption that Eve cannot distinguish between decoy and signal states.

In the appendix, we will show that the optimal $\mu$ for the infinite decoy state case is in the order of 1, $\mu = O(1)$, which yields a final key rate $R = O(\eta)$. On the other hand, the optimal $\mu$ for the non-decoy case is $\mu = O(\eta)$, which yields a final key rate $R = O(\eta^2)$. From here, similar to the coherent state QKD, we expect that the decoy state method can substantially improve the triggering PDC QKD performance.

There are various ways of applying the decoy state idea to the triggering PDC QKD [35]–[37]. Here we consider the upper bound (infinite decoy state case) of all possible decoy state protocols of the triggering PDC QKD with threshold detectors: triggering PDC+infinite decoy state method [19]. In the infinite decoy state method, Alice and Bob perform an infinite number of decoy states by choosing different intensities of the PDC source, $\mu$. Then they can solve the linear equations in the form of equations (7) and (8) for estimating $Y_1$ and $e_1$ accurately. So, they can calculate each $Q_{0,j}$, $Q_{1,j}$, and $e_1$ accurately. In the simulation, we will use equations (10) and (11) directly.

### 4.4. Weak active decoy state with threshold detectors

Here, we assume that Alice and Bob use threshold detectors and focus on triggered detection events. Alice uses another intensity $\nu$, say by attenuating the pumping laser, for the weak decoy state. Wang, Wang and Guo have proposed a practical decoy method for triggering PDC QKD [37], which is essentially applying a vacuum+weak decoy state method [20]. Note that for triggered detection events, the vacuum contribution can be negligible since $\eta_{\mathrm{A}} \gg Y_{0\mathrm{A}}$. Thus, there is no need to estimate the vacuum contribution here. So Alice and Bob only need to perform a weak decoy state instead of vacuum+weak decoy states. In this case, only one weak decoy state is sufficient.

Bounds of $Y_1$ and $e_1$ are given by $\mu^2(1+\nu)^3 \times Q_{\nu,1} - \nu^2(1+\mu)^3 \times Q_{\mu,1}$ in equations (7) and (8)

$$\begin{aligned} Y_1 &\geqslant \frac{1}{\eta_{\mathrm{A}}(\mu-\nu)}\left[\frac{\mu}{\nu}(1+\nu)^3 Q_{\nu,1} - \frac{\nu}{\mu}(1+\mu)^3 Q_{\mu,1}\right], \\ e_1 &\leqslant \min\left\{\frac{(1+\mu)^2}{\mu}\frac{E_{\mu,1}Q_{\mu,1}}{\eta_{\mathrm{A}}Y_1}, \frac{(1+\nu)^2}{\nu}\frac{E_{\nu,1}Q_{\nu,1}}{\eta_{\mathrm{A}}Y_1}\right\}, \end{aligned} \tag{19}$$

where $\nu$ is the expected photon pair number of the weak decoy state and $\eta_A$ is the efficiency of Alice's threshold detector.

It is not hard to show that when $\nu \to 0$, equation (19) approaches the infinite case, equations (10) and (11), described in the previous subsection.

### *4.5. Passive decoy state*

Recently, Mauerer and Silberhorn proposed a passive decoy state scheme, in which photon-number-resolving detectors are required [35]. Let us briefly recapitulate the heuristic idea of the original passive decoy state scheme here. As discussed in section 3, Alice and Bob eventually get different detection events grouped by triggers on Alice's side. The key idea proposed by Mauerer and Silberhorn is that Alice and Bob manually combine the $\{j\}$-trigger detection events to get the decoy states with different photon number statistics and then follow the regular decoy state scheme.

Here we want to point out that the 'combination' step is unnecessary. In general, each detection event group with $j$-trigger has different photon number statistics on the photon source arm. Thus, what Alice and Bob need to do is treat all $\{j\}$-trigger detection events' statistics separately. Furthermore, photon-number-resolving detectors are not necessary in a passive decoys state scheme. Our new generalized passive decoy state scheme is as follows:

1. Alice uses a PDC source as her triggered photon source. She detects one of the modes from her PDC source as triggers and encodes key information into another mode. Due to the detector Alice uses, she will get different trigger events: $j = 0, 1, \ldots$. When she uses a threshold detector, she will only get $j = 0, 1$.
2. As usual for the BB84 protocol, Bob measures signals in two different bases. Alice and Bob perform basis reconciliation.
3. Alice announces her trigger-detection results for each pulse: $j$. Bob groups his detection events by the information $j$. For each $j$, they calculate the gain $Q_{\mu,j}$ and test the QBER $E_{\mu,j}$.
   Mathematically, they will obtain a set of linear equations in the form of equations (7) and (8). Notice that the setup parameters, $\mu$ and $\eta_{j|i}$s, are known to Alice and Bob. Thus, they can estimate $Y_1$ and $e_1$ by considering equations (7) and (8).
4. Apply post-processing according to equation (16).

We remark that the scheme is called *passive* because Alice does not actively select decoy states. Instead, she determines the decoy states by measuring the trigger mode. Later, we will show that this is one advantage of using a triggering PDC source for QKD. Actually, in this case, there is no strict definition of decoy and signal states. In the original decoy state method [20], decoy states are only used for estimating $Y_1$ and $e_1$ and the key is always generated from signal states[7]. In the triggering PDC QKD case, both the triggered $j = 0$ and non-triggered $j = 1$ detection events may have positive contribution to the final key generation.

[7] In the coherent state QKD, there is an optimal $\mu$ for a setup. To maximize the final key rate, Alice and Bob should publicly compare all detection results from decoy states.

### *4.6. Passive decoy state with threshold detectors*

Here, we will review the decoy state protocol proposed by AYKI [36] as a special case of the passive decoy state protocol. The AYKI protocol is interesting in practice since it does not involve any hardware change for implementing decoy states.

Both Alice and Bob use threshold detectors, thus they have two types of detection events, triggered ($j = 1$) and non-triggered ($j = 0$). Secure keys can be generated from both types of detection events. Following the passive decoy state method procedure described in the previous subsection, Alice and Bob can estimate $Y_1$ and $e_1$ by considering the statistics of triggered and non-triggered detection events separately. This is conceptually similar to one decoy state idea [20].

By solving two linear equations of equation (7) with $j = 0, 1$, $[1-(1-\eta_A)^2] \times Q_{\mu,0} - (1-\eta_A)^2 \times Q_{\mu,1}$, one obtains

$$Y_1 \geqslant Y_1^L \equiv \frac{(1+\mu)^2}{\mu}\left[\frac{2-\eta_A}{1-\eta_A}(Q_{\mu,0}-Q_{0,0}) - \frac{1-\eta_A}{\eta_A}Q_{\mu,1}\right], \tag{20}$$

where $Q_{0,0}$ is the vacuum state contribution in non-triggered detection events. One needs to minimize the key rate of equation (16) for $Q_{0,0}$ with the constraint of equations (7) and (8). We note that this result is essentially the equation (14) given in [36]. We can see that when $\eta_A$ is close to 1 or $\mu$ is small, after neglecting $Q_{\mu,0}$ (background counts), the lower bound $Y_1^L$ is tight (approaches the real value of $Y_1$, see equation (4)),

$$\lim_{\eta_A \to 1} Y_1^L = \lim_{\mu \to 0} Y_1^L = \eta. \tag{21}$$

By neglecting the vacuum state contribution for triggered detection events, $Q_{0,1} = 0$, $e_1$ can be simply estimated by

$$e_1 \leqslant \frac{E_{\mu,1}Q_{\mu,1}}{Q_{1,1}}. \tag{22}$$

To get the lower bound of $Y_1$ in equation (20), one has to estimate the background contribution $Q_{0,0}$ as well. One simple bound of $Q_{0,0}$ is $0 \leqslant e_0 Q_{0,0} \leqslant E_{\mu,0} Q_{\mu,0}$ from equation (8), where $e_0 = 1/2$.

We note that the key rate calculated by substituting equations (20) and (22) into equation (16) is not optimal. To get a tighter key rate bound, one can numerically lower bound equation (16) directly given the measurement results, equation (11).

### *4.7. With a perfect photon-number-resolving detector*

Here, we discuss a special case that Alice uses a perfect photon-number-resolving detector, discussed in section 3.4. Now that Alice knows the exact photon number of the source, Alice and Bob only need to focus the post-processing on the single photon-state detection events. In this case, the BB84 protocol is implemented by single photon states only. Thus, they can directly apply Shor and Preskill's formula [5, 34]

$$R \geqslant q Q_1[1 - f(e_1)H_2(e_1) - H_2(e_1)]. \tag{23}$$

Later from the simulation, shown in figure 2, we can see that a perfect photon-number-resolving detector does not improve the QKD performance much compared with the threshold detector case.

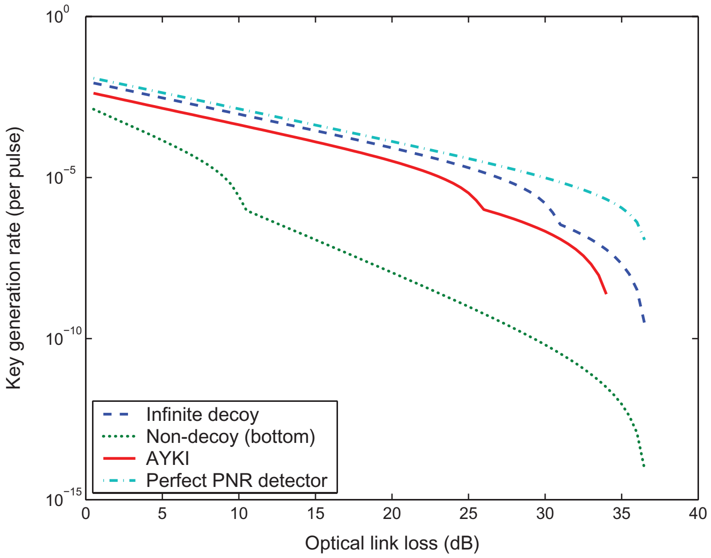

**Figure 2.** Plot of the key generation rate in terms of the optical loss, comparing four schemes without considering statistical fluctuations: non-decoy, infinite decoy, AYKI and the case with a perfect number-resolving detector. Here, we use $q = 1/2$ and $f(E_\mu) = 1.22$. We numerically optimize $\mu$ for each curve, see appendix for more discussions. Simulation parameters are listed in table 1.

**Table 1.** List of parameters from 144 km PDC experiment [39]. Here $\eta_A$ and $\eta_{Bob}$ are the detection efficiencies in Alice and Bob's detection system, not including the optical channel loss. $e_d$ is the intrinsic detector error rate. $Y_{0B}$ is the background count rate of Bob's detection system (for example, if Bob has two detectors, then $Y_{0B}$ will be the sum of two detectors' background count rates). The transmission efficiency $\eta$ in equation (4) is given by $\eta_{Bob}$ plus the channel loss.

| Frequency | Wavelength | $\eta_A$ | $\eta_{Bob}$ | $e_d$ | $Y_{0B}$ |
|---|---|---|---|---|---|
| 249 MHz | 710 nm | 14.5% | 14.5% | 1.5% | $6.024 \times 10^{-6}$ |

### 4.8. A few remarks

From the analysis of optimal $\mu$ in the appendix, one can see that the key rate for the case without decoy states quadratically depends on the channel loss, $R = O(\eta^2)$, while for the case with decoy states, $R = O(\eta)$. This result is consistent with prior work in comparing the cases of coherent state QKD with and without decoy states [19].

In the decoy state security proof [19], the key assumption is that the decoy and signal states should satisfy equation (18). This is guaranteed by the assumption that Eve cannot distinguish between decoy and signal states. However, in the active decoy state method, Alice may introduce side information that can distinguish decoy and signal states when she actively prepares decoy and signal states. For example, an attenuator on Alice's side, used for preparing different intensities for signal and decoy states, may introduce different frequency shifts for signal and decoy states [24]. In general, it is hard to verify the assumption that Eve cannot distinguish decoy and signal states in real active decoy state experiments.

In the passive decoy state scheme, decoy and signal states are passively determined by Alice's measurement outcome. Alice does not use an extra component (like in the active decoy state method) for preparing decoy states. This reduces the possibility of side information leakage. By passively choosing decoy states, Alice prepares the same states on Bob's arm[8]. In fact, Alice can measure trigger signals after Bob finishes his measurements. Thus, from Eve's point of view, the states transmitted through the channel are independent of Alice's measurement results ($j$). Therefore, in principle, Eve cannot distinguish the decoy and signal states in the passive decoy state QKD[9]. This is one advantage of using passive decoy state methods. Note that for the coherent state QKD, one can only use active decoy state methods.

## 5. Simulation

In this section, we will compare the passive decoy state with a perfect number-resolving detector and four QKD implementations with threshold detectors: non-decoy, infinite decoy, weak active decoy and AYKI (weak passive decoy state). Note that the simulation of AYKI was done in [36] and the one of weak active decoy state method was done in [37].

The model for the simulation is given in section 3. All the simulation results are calculated by equations (15) and (16). The estimations of the parameters for each method are discussed in section 4.

We deduce experimental parameters from a recent PDC experiment [39], which are listed in table 1. In the following simulations, we will use $q = 1/2$ and $f(E_\mu) = 1.22$ in equation (15). We notice that with the slightly modified experimental setup, a coherent state QKD with decoy states has been implemented [39]. Thus, it is reasonable to use this experimental setup for simulating the five QKD implementations.

In the simulation, for fair comparison, we assume Bob uses the same detection setup (with threshold detectors) for all cases.

### *5.1. Without statistical fluctuations*

In the first simulation, we consider the case in which Alice and Bob perform an infinitely long QKD (no statistical fluctuations). In this case, the weak active decoy state protocol converges the infinite decoy case [20]. We assume that Alice is able to adjust $\mu$ (the brightness of the PDC source) in the regime of [0, 1], arbitrarily. In the simulation, we numerically optimize $\mu$ for each of the four implementation protocols: non-decoy, infinite decoy, AYKI and the case with a perfect number-resolving detector. The simulation result is shown in figure 2.

From figure 2, we have the following remarks:

1. In the appendix, instead of numerically optimizing $\mu$ as done for figure 2, we qualitatively investigate the optimal $\mu$ for triggering PDC QKD with and without decoy states. The simulation result is consistent with the qualitative conclusion $R = O(\eta)$ for the case with decoy state and $R = O(\eta^2)$ for the case without decoy state.
2. The space between the solid and dashed lines in figure 2 indicates the room left for improvement by other decoy state protocols with threshold detectors after the AYKI

[8] Strictly speaking, there is one underlying assumption: the PDC source is single-mode.

[9] The underlying assumption here is that from Eve's point of view, the pulses emitted from the PDC source are identical and independent.

protocol is implemented. We can see that, in a large regime of the optical link loss, the performances of AYKI and the infinite decoy are close. For instance, the AYKI protocol yields around 50% of the key rate of the infinite decoy state protocol when the channel loss is within 20 dB.

3. By comparing AYKI and the case with a perfect photon-number-resolving detector, we can see that even with a perfect photon-number-resolving detector on Alice's side, the key rate is not improved much in a large regime of the optical loss.
4. The non-decoy state protocol is better than AYKI in the regime nearby the maximal secure distances. This is because we use the bounds of equations (20) and (22) for the AYKI curve. In reality, Alice and Bob can use the bound of equation (17) directly in this regime.
5. There is a bump in each curve. This is due to the fact that in the key generation rate formula equation (16), the non-triggered detection events have no contribution to the final secure key after the bump.
6. At the point of loss $= 0$ dB, the key rates of four cases (from the top to the bottom) are $1.21 \times 10^{-2}$, $8.6 \times 10^{-3}$, $4.2 \times 10^{-3}$ and $1.3 \times 10^{-3}$.
7. At the point of loss $= 0$ dB, the numerical results for optimal $\mu$ for four cases (from the top to the bottom) are: 1, 0.52, 0.194 and 0.0589. The optimal $\mu$ for the case with a perfect threshold detector is always 1, which is reasonable since $\mu = 1$ maximizes the single photon state probability. In the appendix, we show that the optimal $\mu$s for the infinite decoy and AYKI cases are relatively stable in a large regime of the optical loss. The optimal $\mu$ for the no decoy state case decreases with channel loss.
8. In a real PDC experiment, the abovementioned $\mu \approx 1$ or 0.5 may not be achievable. The real $\mu$ used in the experiment [39] is $\mu = 0.053$. We have also compared various protocols by using the real $\mu = 0.053$ and drawn similar conclusions.
9. All of the four cases can tolerate similar optical losses.

### 5.2. *With statistical fluctuations*

In a real experiment, the key length is always finite. Alice and Bob should consider statistical fluctuations. As pointed in [20], statistical fluctuation analysis is a complicated problem in the decoy state QKD. Similar to the analysis in [20], we assume a few conditions:

1. Alice knows the exact value of average photon pair number $\mu$, which is a fixed number during key transmission.
2. The distribution of photon number, (3), does not fluctuate.
3. We assume the QKD transmission is part of an infinite length experiment. Then, we assume the real measurement results, the gain $Q_{\mu,j}$ and the QBER $E_{\mu,j}$, follows a normal distribution centred in the expected values (in the infinite length experiment). Here, we skip all the tedious mathematical formulae for the fluctuation analysis. For detailed calculations, one may refer to [20].

Here, we focus on the three cases with threshold detectors: infinite decoy, weak decoy and AYKI. We assume that the data size is $6 \times 10^9$ pulses of Alice's pumping laser. The simulation result is shown in figure 3. From the simulation result, we have the following observations:

1. Similar to the case without fluctuation analysis, in a large regime of the optical link loss, the performances of AYKI and the infinite decoy are close.

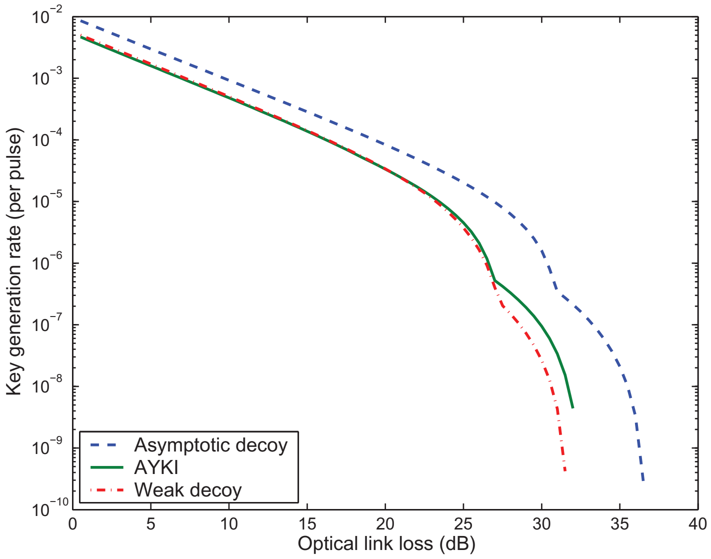

**Figure 3.** Plot of the key generation rate in terms of the optical loss, comparing three cases with threshold detectors after considering statistical fluctuations: infinite decoy, weak active decoy and AYKI. We numerically optimize $\mu$ for each curve. Here, we use $q = 1/2$ and $f(E_\mu) = 1.22$. In the weak decoy state case, we assume Alice can randomly attenuate her PDC source intensity. Simulation parameters are listed in table 1. The data size is $6 \times 10^9$ pumping laser pulses on Alice's side.

2. At the point of loss = 0 dB, the key rates of the three cases from the top to the bottom are $8.6 \times 10^{-3}$ (infinite), $5.0 \times 10^{-3}$ (weak) and $4.7 \times 10^{-3}$ (AYKI).
3. The maximal tolerable secure optical losses for the three cases are rather similar: 37 dB (infinite), 32.5 dB (AYKI) and 32 dB (weak).
4. The AYKI protocol yields a higher key rate than weak decoy state protocol when the loss is greater than 16 dB. AYKI is less affected by statistical fluctuations than the weak decoy state because in AYKI, Alice does not need to sacrifice extra pulses for decoy states.

In section 4.8, we have pointed out that from a practical security point of view, the passive decoy state method has an advantage over active decoy state methods. Also, the AYKI method does not require any additional hardware change for implementing a decoy state, whereas in the weak decoy state case, Alice needs to add an attenuator for creating decoy states. Now, from the simulation results, we can see that AYKI and weak active decoy state methods yield similar QKD performance. Thus, our conclusion is that one should just use the AYKI method instead of the weak decoy state method.

## 6. Conclusion

By investigating the optimal photon source intensity, we find that the triggering PDC QKD setup with decoy states is able to achieve a key rate that linearly depends on the channel transmittance, compared with the quadratic dependence for the case without decoy states. Therefore, we expect the decoy state QKD to become a standard technique not only in the coherent state QKD, but also in QKD with triggering PDC sources.

On the practical side, we generalize the passive decoy state idea. The generalized passive decoy state idea can be applied to cases where either threshold detectors or photon-number-resolving detectors are used. The decoy state protocol proposed by AYKI can be treated as a special case of the generalized passive decoy state method. Comparing with the active (regular) decoy state methods, the passive one opens a lower possibility for Eve to distinguish between decoy and signal states, which is a key underlying assumption in the security proof of decoy state QKD. From this sense, the passive decoy state method is more secure than the active decoy state methods in practice.

By simulating a recent PDC experiment, we compare various practical decoy state protocols with the infinite decoy state protocol. We also compare the cases using threshold detectors and photon-number-resolving detectors. Our simulation result shows that with the AYKI protocol, one can achieve a key generation rate that is close to the theoretical limit of the infinite decoy state protocol. Furthermore, our simulation result suggests that a photon-number-resolving detector has a minor advantage, compared with the case using threshold detectors, in terms of the QKD performance.

We also consider the statistical fluctuations. We compare the infinite decoy state protocol, weak active decoy state method and AYKI protocol. The simulation result shows that the weak active decoy state method and AYKI protocol yield very close QKD performance. In a large regime of the optical loss, the AYKI protocol can achieve a performance that is close to the infinite decoy case. Since the AYKI protocol requires no hardware changes for triggering PDC QKD, we conclude that the AYKI method is a good protocol for triggering PDC QKD experiments.

Although our analysis is focused on the QKD with PDC sources, we emphasize that it can also be applied to QKD setups with other triggered single photon sources.

## Acknowledgments

We thank C-H F Fung, W Mauerer, A M Steinberg, G Weihs and X Xing for their enlightening discussions. For the simulation part, we thank H Hübel for confirming the parameters we deduced from their experiments. This work has been supported by the CFI, CIFAR, CIPI, Connaught, CRC, MITACS, NSERC, OIT, PREA, QuantumWorks and the University of Toronto. XM acknowledges the Chinese Government Award for Outstanding Self-financed Students Abroad and the Lachlan Gilchrist Fellowship.

## Appendix. Optimal $\mu$

The optimal $\mu$ for the coherent state QKD with and without decoy states has already been studied [20]. Here, instead of numerically optimizing $\mu$ as done for figure 2, we qualitatively investigate the optimal $\mu$ for the triggering PDC QKD with and without decoy states. Here, we are interested in the case that Alice uses a threshold detector.

### *A.1. Without decoy states*

Let us begin with the optimal $\mu$ of the case without decoy states. Here we will apply GLLP [12] security analysis. As shown in [54], GLLP and Lütkenhaus's [8] security analyses achieve

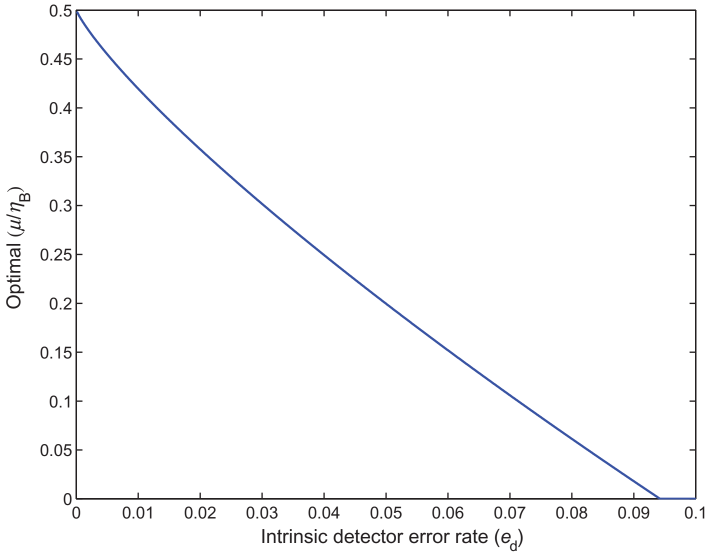

**Figure A.1.** Plot of the optimal $\mu$ in terms of $e_\mathrm{d}$ for triggering PDC+non-decoy. Here we use $f(e_\mathrm{d}) = 1.22$, since the error rate is less than 10% [52].

similar performances for the coherent state QKD. Intuitively, we should get a similar optimal $\mu$ as given in [8], $\mu \approx \eta/2$.

From equation (10), we can see that the gain $Q_{\mu,j}$ $(j = 0, 1)$ is in the order of $\mu\eta$. To keep $Q_{1,0}$ or $Q_{1,1}$ in equation (17) positive, $\mu$ should be in the order of $\eta$. By assuming $\mu$, $\eta$ and $Y_{0\mathrm{B}}$ are small, we can simplify equation (10)

$$\begin{aligned} &Q_{\mu,0} + Q_{\mu,1} \approx \eta\mu, \\ &E_{\mu,0} \approx E_{\mu,1} \approx e_\mathrm{d}, \\ &Q^\mathrm{L}_{1,0} + Q^\mathrm{L}_{1,1} \approx \eta\mu - \mu^2, \\ &e^\mathrm{U}_1 \approx \frac{\eta e_\mathrm{d}}{\eta - \mu}, \end{aligned} \tag{A.1}$$

where $Q^\mathrm{L}_{1,0} + Q^\mathrm{L}_{1,1}$ is the lower bound of $Q_{1,0} + Q_{1,1}$, and $e^\mathrm{U}_1$ is the upper bound of $e_1$ from equation (17). Since the error rates from triggered $(j = 1)$ and non-triggered $(j = 0)$ detection events are the same, the key generation rate given by equation (13) can be simplified to

$$\begin{aligned} R \geqslant& q\{-f(E_\mu)Q_\mu H_2(E_\mu) + Q_1[1 - H_2(e_1)] + Q_0\} \\ \approx& q\left\{-f(e_\mathrm{d})\eta\mu H_2(e_\mathrm{d}) + (\eta\mu - \mu^2)\left[1 - H_2\left(\frac{\eta e_\mathrm{d}}{\eta - \mu}\right)\right]\right\}. \end{aligned} \tag{A.2}$$

By taking derivative of $R$, the optimal $\mu \equiv x\eta$ satisfies

$$-f(e_\mathrm{d})H_2(e_\mathrm{d}) + 1 - 2x + e_\mathrm{d}\log_2\frac{e_\mathrm{d}}{1-x} + (1 - e_\mathrm{d} - 2x)\log_2\left(1 - \frac{e_\mathrm{d}}{1-x}\right) = 0. \tag{A.3}$$

Here if we set $e_\mathrm{d} = 0$, then we get $x = 1/2$ which is compatible with Lükenthaus' result [8]. We note that $x = 1/2$ essentially maximizes the probability of single photon source $Q^\mathrm{L}_{1,0} + Q^\mathrm{L}_{1,1}$ in equaton (A.1). More precisely, we can solve equation (A.3) numerically, see figure A.1.

From figure A.1, we can see that the optimal $\mu$ for triggering PDC+non-decoy is $\mu = O(\eta)$, which will lead the final key generation rate $R = O(\eta^2)$.

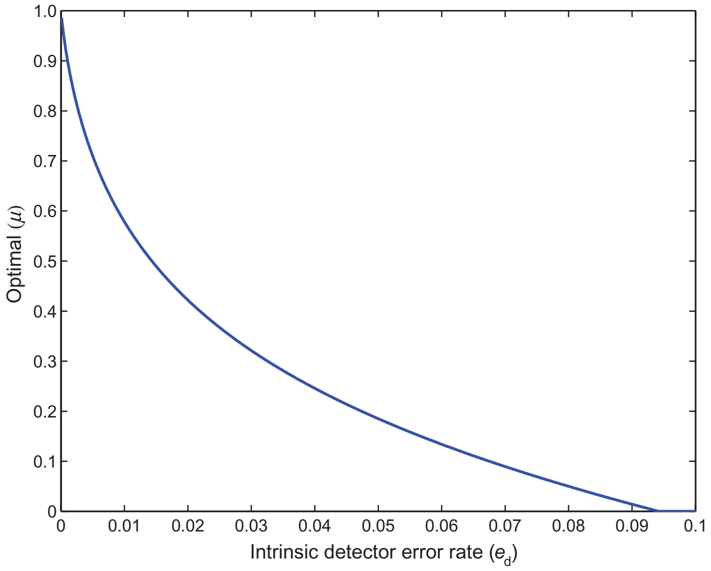

**Figure A.2.** Plot of the optimal $\mu$ in terms of $e_d$ for the triggering PDC+infinite decoy. Here, we use $f(e_d) = 1.22$.

### *A.2. With decoy states*

With decoy states, Alice and Bob can estimate $Q_1$ and $e_1$ better. Here we consider the infinite decoy state case with threshold detectors. Under the assumption that $\eta$ and $Y_{0B}$ are small, we can simplify equations (10) and (11),

$$\begin{aligned} &Q_{\mu,0} + Q_{\mu,1} \approx \eta\mu, \\ &E_{\mu,0} \approx E_{\mu,1} \approx e_d, \\ &Q_{1,0} + Q_{1,1} \approx \frac{\eta\mu}{(1+\mu)^2}, \\ &e_1 \approx e_d. \end{aligned} \tag{A.4}$$

With these approximations, the key generation rate given in equation (13) can be simplified to

$$R \approx q\left\{-f(e_d)\eta\mu H_2(e_d) + \frac{\eta\mu}{(1+\mu)^2}[1 - H_2(e_d)]\right\}. \tag{A.5}$$

The optimal $\mu$ satisfies

$$\frac{1-\mu}{(1+\mu)^3} = \frac{f(e_d)H_2(e_d)}{1-H_2(e_d)}. \tag{A.6}$$

Here, if we set $e_d = 0$, then we get $\mu = 1$ with which the probability of getting a single photon state is maximized. The numerical result of equation (A.6) is shown in figure A.2.

From figure A.2, similar to the case of coherent state QKD with decoy states [20], one can see that the optimal $\mu$ is (almost) independent of channel loss $\eta$ for the infinite decoy state case with threshold detectors, i.e. $\mu = O(1)$, which will lead to the final key generation rate $R = O(\eta)$.

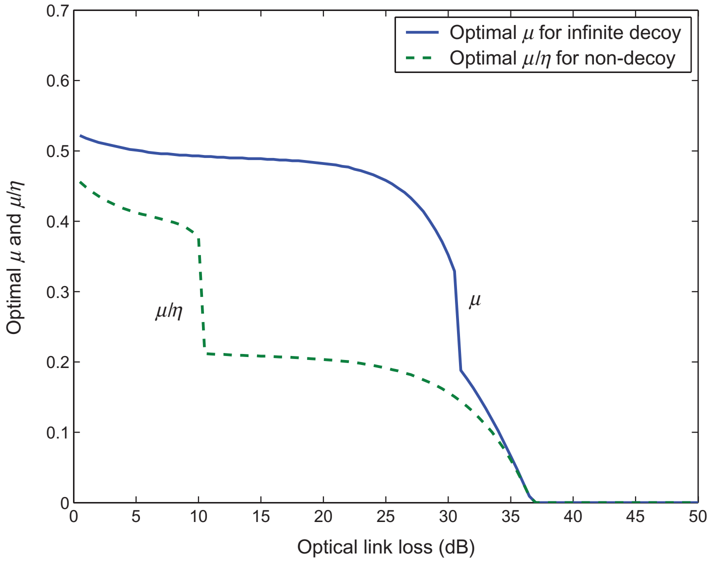

**Figure A.3.** Plot of the optimal $\mu$ in terms of optical loss for triggering PDC+non-decoy and triggering PDC+infinite-decoy. Here, we use $q = 1/2$ and $f(E_\mu) = 1.22$. Simulation parameters are listed in table 1.

### *A.3. Numerical checking*

Now we would like to numerically compare the optimal $\mu$ with and without decoy states by simulating a recent PDC experiment [39], with parameters listed in table 1. In the simulation, we numerically optimize $\mu$ for the key rate given by equation (16) for the non-decoy and infinite decoy methods. For this particular setup, the optimal $\mu$ is shown in figure A.3.

From the figure, we can see that the optimal $\mu$ for the non-decoy case is in the order of $\eta$, while the optimal $\mu$ for the infinite-decoy case is in the order of 1. This is consistent with the results of the analysis presented in the two previous subsections.

## References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing Bangalore, India* (New York: IEEE) pp 175–9
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Mayers D 2001 *J. ACM* **48** 351–406
[4] Lo H-K and Chau H-F 1999 *Science* **283** 2050
[5] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[6] Koashi M 2006 *J. Phys.: Conf. Ser.* **36** 98
[7] Mayers D and Yao A 1998 *FOCS, 39th Annu. Symp. on Foundations of Computer Science* (Los Alamitos: IEEE, Computer Society Press) p 503
[8] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304
[9] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[10] Inamori H, Lütkenhaus N and Mayers D 2007 *Eur. Phys. J.* D **41** 599
[11] Koashi M and Preskill J 2003 *Phys. Rev. Lett.* **90** 057902
[12] Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 *Quantum Inform. Comput.* **4** 325
[13] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J A 1992 *J. Cryptol.* **5** 3
[14] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev.* A **51** 1863

[15] Lütkenhaus N and Jahma M 2002 *New J. Phys.* **4** 44

[16] Hwang W-Y 2003 *Phys. Rev. Lett.* **91** 057901

[17] Lo H-K 2004 *Proc. IEEE ISIT* (New York: IEEE) p 137

[18] Ma X 2004 *Preprint* quant-ph/0503057

[19] Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[20] Ma X, Qi B, Zhao Y and Lo H-K 2005 *Phys. Rev.* A **72** 012326

[21] Harrington J W, Ettinger J M, Hughes R J and Nordholt J E 2005 *Preprint* quant-ph/0503002

[22] Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503

[23] Wang X-B 2005 *Phys. Rev.* A **72** 012322

[24] Zhao Y, Qi B, Ma X, Lo H-K and Qian L 2006 *Phys. Rev. Lett.* **96** 070502

[25] Zhao Y, Qi B, Ma X, Lo H-K and Qian L 2006 *Proc. IEEE ISIT* (New York: IEEE) p 2094

[26] Rosenberg D, Harrington J W, Rice P R, Hiskett P A, Peterson C G, Hughes R J, Lita A E, Nam S W and Nordholt J E 2007 *Phys. Rev. Lett.* **98** 010503

[27] Schmitt-Manderbach T *et al* 2007 *Phys. Rev. Lett.* **98** 010504

[28] Peng C-Z, Zhang J, Yang D, Gao W-B, Ma H-X, Yin H, Zeng H-P, Yang T, Wang X-B and Pan J-W 2007 *Phys. Rev. Lett.* **98** 010505

[29] Yuan Z L, Sharpe A W and Shields A J 2007 *Appl. Phys. Lett.* **90** 011118

[30] Koashi M 2004 *Phys. Rev. Lett.* **93** 120501

[31] Tamaki K, Lütkenhaus N, Koashi M and Batuwantudawe J 2006 *Preprint* quant-ph/0607082

[32] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902

[33] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[34] Ma X, Fung C-H F and Lo H-K 2007 *Phys. Rev.* A **76** 012307

[35] Mauerer W and Silberhorn C 2007 *Phys. Rev.* A **75** 050305

[36] Adachi Y, Yamamoto T, Koashi M and Imoto N 2007 *Phys. Rev. Lett.* **99** 180503

[37] Wang Q, Wang X-B and Guo G-C 2007 *Phys. Rev.* A **75** 012312

[38] Wang Q, Wang X-B, Björk G and Karlsson A 2007 *Europhys. Lett.* **79** 40001

[39] Ursin R *et al* 2007 *Nat. Phys.* **3** 481

[40] Walls D F and Milburn G J 1994 *Quantum Optics* (Berlin: Springer)

[41] Sergienko A V, Atatüre M, Walton Z, Jaeger G, Saleh B E A and Teich M C 1999 *Phys. Rev.* A **60** R2622

[42] Brassard G, Mor T and Sanders B C 1999 *Preprint* quant-ph/9906074

[43] Jennewein T, Simon C, Weihs G, Weinfurter H and Zeilinger A 2000 *Phys. Rev. Lett.* **84** 4729

[44] Boyd R 2002 *Nonlinear Optics* 2nd edn (New York: Academic)

[45] Scarani V, Acin G R A and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901

[46] Tamaki K and Lo H-K 2006 *Phys. Rev.* A **73** 010302

[47] Koashi M 2006 *Preprint* quant-ph/0609180

[48] Tsurumaru T and Tamaki K 2008 *Preprint* 0803.4226

[49] Beaudry N J, Moroder T and Lütkenhaus N 2008 *Preprint* 0804.3082

[50] Lo H-K 2005 *Quantum Inform. Comput.* **5** 413

[51] Lo H-K, Chau H-F and Ardehali M 2005 *J. Cryptol.* **18** 133

[52] Brassard G and Salvail L 1993 *Advances in Cryptology EUROCRYPT '93* ed G Goos and J Hartmanis (Berlin: Springer)

[53] Ma X, Fung C-H F, Dupuis F, Chen K, Tamaki K and Lo H-K 2006 *Phys. Rev.* A **74** 032330

[54] Ma X 2006 *Phys. Rev.* A **74** 052325