Secure quantum key distribution in an easy way

Jia-Zhong Hu¹ and Xiang-Bin Wang¹,

¹Department of Physics, Tsinghua University, Beijing 100084, China

Abstract

Secure quantum key distribution can be achieved with an imperfect single-photon source through implementing the decoy-state method. However, security of all those theoretical results of decoy-state method based on the original framework raised by Hwang needs monitoring the source state very carefully, because the elementary proposition that the counting rates of the same state from different sources are equal does not hold in general when the source is unstable. Source intensity monitoring greatly decreases the system efficiency. Here without using Hwang’s proposition for stable source, we present a sufficient condition for a secure decoy-state protocol without monitoring the source intensity. The passive 2-intensity protocol proposed by Adachi, Yamamoto, Koashi, and Imoto(AYKI) (Phys. Rev. Lett. 99, 180503 (2007) ) satisfies the condition. Therefore, the protocol can always work securely without monitoring the source state or switching the source intensity. We also show that our result can greatly improve the key rate of the 3-intensity protocol with a fluctuating coherent-state source.

PACS numbers: 03.67.Dd, 42.81.Gs, 03.67.Hk

*Electronic address: xbwang@mail.tsinghua.edu.cn
I. INTRODUCTION

Imperfect single-photon source is used in most of the existing set-ups of quantum key distribution (QKD)[1–3]. To make it secure even under photon-number-splitting attack[4, 5], one can use the decoy-state method[7–13] based on the general theory of QKD with an imperfect source which was first built by Inamori, Lütkenhaus and Mayers[3] and then further studied with some improved results[6]. There are also some other methods[14, 15] which can make secure QKD with an imperfect source.

Though many experiments on the decoy-state QKD have been done[16], the original decoy-state theory[8–10] assumes perfect control of the source states in the photon number space. This is an impossible task for any real set-up in practice. A new non-trivial problem arises in practice is how to carry out the decoy-state method securely and efficiently with an unstable source.

The most important proposition of the decoy-state method given by Hwang[8] is

\[ s_k = s'_k \]  

where \( s_k \) and \( s'_k \) are the yield (counting rate) of those \( k \)-photon pulses from the decoy source and that from the signal source. However, as pointed out in Ref.[7, 19, 20] with concrete examples that this elementary proposition does not always hold for a fluctuating source. (Note that the fluctuation of each individual pulses are in general not independent.)

To solve this problem, a number of theoretical works have been done[17–22]. In particular, without using Eq.(1), a general formula was given in Ref.[19] for the 3-intensity decoy-state method with whatever type of error pattern in the source, if we can monitor the range of a few parameters of each individual pulse state out of Alice’s lab. Although source monitoring can be done with the existing technology by detecting the intensity of a strong father pulse in the beginning[23, 24], it will raise the cost of the real QKD system and decrease the outcome efficiency because the repetition rate of strong pulse detection is low. Therefore, it is a meaningful job to find a class of decoy-state protocols which can work securely without monitoring any source fluctuation.

Here, without using Eq.(1), we shall give the condition that a decoy state protocol can work securely with a fluctuating source. We then show that the 2-intensity passive protocol proposed by Adachi, Yamamoto, Koashi, and Imoto (AYKI)[12] meets the condition of our theorem.
In what follows, we shall first derive an improved formula for a 2-intensity decoy-state protocol with source fluctuation. Based on this, we propose a theorem on the condition for a protocol to work securely without source monitoring. Directly applying the theorem we find AYKI protocol meets the condition and the main formula in AYKI protocol is independent of whatever source intensity fluctuation. We then extend our formula to the 3-intensity protocol and show its high efficiency for a coherent-state based protocol with numerical simulation.

II. OUR THEOREM AYKI PROTOCOL

In a 2-intensity protocol, Alice has 2 (virtual) sources, the decoy source $Y$ which prepares decoy pulses, and the signal source $Y'$ which prepares signal pulses. At any time $i$, each source prepares a pulse and Alice randomly choose one of them sending out to Bob. Suppose at any time $i$ Alice has a probability $p_i$, $p_i'$ to sends out the pulse from source $Y$ and $Y'$, respectively ($p_i + p_i' = 1$). Note that $p_i$, $p_i'$ are not necessarily constant values here. Denote $\rho_i$, $\rho_i'$ as state of a decoy pulse and that of a signal pulse produced at the $i$th time:

$$\rho_i = \sum_{k=0}^{J} a_{ki} |k\rangle \langle k| ; \quad \rho_i' = \sum_{k=0}^{J} a_{ki}' |k\rangle \langle k|.$$  \hspace{1cm} (2)

Here $J$ can be either finite or infinite.

Definitely, it makes no difference if all pulses sent out to Bob are actually produced by only one physical source. But we assume there are two sources for clarity in presentation.

In the whole protocol, Alice sends Bob $M$ pulses, one by one. In response to Alice, Bob observes his detector for $M$ times. As Bob’s $i$th observed result, Bob’s detector can either click or not click. If the detector clicks in Bob’s $i$th observation, then we say that “the $i$th pulse from Alice has caused a count”. We disregard how the $i$th pulse may change after it is sent out. When we say that Alice’s $i$th pulse has caused a count we actually mean that pulse is accompanied by a click at Bob’s side at Bob’s $i$th observation.

Given the source state in Eqs.(2), any $i$th pulse sent out by Alice must be in a specific photon-number state. To anyone outside Alice’s lab, it looks as if that Alice only sends a photon number state at each time $i$: sometimes it’s vacuum, sometimes it’s a single-photon pulse, sometimes it is a 2–photon pulses, and so on. We shall make use of this fact that any individual pulse is in one Fock state. On the other hand, pulses sent out to Bob can also be
classified by which source it comes from, i.e., a decoy pulse if it is from the decoy source or a signal pulse if it is from the signal source.

Given Eqs. (2), we have the following formulas for \( P_{\text{di} | k} \) and \( P_{\text{si} | k} \), the probabilities that the \( i \)th pulse comes from the decoy source or signal source; if the \( i \)th pulse contains \( k \) photons:

\[
P_{\text{di} | k} = p_i a_{ki} d_{ki}, \quad P_{\text{si} | k} = p'_i a'_{ki} d_{ki}
\]

where

\[
d_{ki} = \frac{1}{p_i a_{ki} + p'_i a'_{ki}}, \quad \text{for } k \geq 0.
\]

Based on these, we can build up equations which lead to lower bound of the number of single-photon counts.

### A. Definitions

We postulate some definitions first: Set \( \Omega = \{ i = 1, 2, \ldots, M \} \), it contains all \( i \). Set \( C \) contains any pulse that has caused a count; set \( c_k \) contains any \( k \)-photon pulse that has caused a count. Mathematically, the sufficient and necessary condition for \( i \in C \) is that the \( i \)th pulse has caused a count. The sufficient and necessary condition for \( i \in c_k \) is that the \( i \)th pulse contains \( k \) photons and it has caused a count. For instance, if the photon number states of the first 10 pulses from Alice are \( |0\rangle, |0\rangle, |1\rangle, |2\rangle, |0\rangle, |1\rangle, |3\rangle, |2\rangle, |1\rangle, |0\rangle \), and the pulses of \( i = 2, 3, 5, 6, 9, 10 \) each has caused a count at Bob’s side, then we have

\[
C = \{ i | i = 2, 3, 5, 6, 9, 10, \ldots \}; \quad c_0 = \{ i | i = 2, 5, 10, \ldots \}; \quad c_1 = \{ i | i = 3, 6, 9, \ldots \}.
\]

The number of counts caused by \( k \)-photon pulse \( n_k \) is just the number of elements in set \( c_k \). We shall use notation \( n_{kd}, n_{ks} \) for the the number of counts caused by a \( k \)-photon decoy pulse and a \( k \)-photon signal pulse, respectively. These numbers cannot be directly observed in the experiment. Obviously, \( n_{kd} + n_{ks} = n_k \). Suppose in the whole protocol, there are \( N_d \) counts caused by decoy pulses and \( N_s \) counts caused by signal pulses. Note that \( N_d \) and \( N_s \) can be directly observed in the protocol therefore we regard them as known values. Our goal is to find a formula for \( n_{1s} \), i.e., to formulate \( n_{1s} \) by \( n_{0s}, n_{0d} \) and the known values \( N_d, N_s \) and the bound values of the parameters in the decoy state and signal state of Eq. (2). (In a 2-intensity protocol, values of \( n_{0d} \) or \( n_{0s} \) is unknown, but one can still calculate the final key rate with worst-case estimation\[10, 12\].)
B. Derivation of Main Formulas

With definitions postulated earlier, we have

\[ N_d = \sum_{k=0}^{J} n_{kd}, \quad N_s = \sum_{k=0}^{J} n_{ks} \]  \hspace{1cm} (6)

Asymptotically,

\[ n_{kd} = \sum_{i \in c_k} p_i a_{i1} d_{i1}; \quad n_{ks} = \sum_{i \in c_k} p_i a'_{i1} d_{i1} \]  \hspace{1cm} (7)

Consequently,

\[ N_d = n_{0d} + \sum_{i \in c_1} p_i a_{i1} d_{i1} + \sum_{k=2}^{J} \sum_{i \in c_k} p_i a_{ki} d_{ki}, \]  \hspace{1cm} (8)

\[ N_s = n_{0s} + \sum_{i \in c_1} p'_i a'_{i1} d_{i1} + \sum_{k=2}^{J} \sum_{i \in c_k} p'_i a'_{ki} d_{ki}. \]  \hspace{1cm} (9)

We want to find the lower bound of value \( n_{1s} \). Recall the definition of \( d_{ki} \) in Eq.(4), we have

\[ n_{1s} = \sum_{i \in c_1} p'_i a'_{i1} d_{i1} \geq \tilde{N}_{1s} = \sum_{i \in c_1} \frac{1}{1 + \max_{i \in c_1} \left( \frac{p_i a_{i1}}{p'_i a'_{i1}} \right)} \]  \hspace{1cm} (10)

Eqs.(8, 9) can be written in

\[ N_d = n_{0d} + \max_{j \in c_1} \left( \frac{p_j a_{j1}}{p'_j a'_{j1}} \right) \tilde{N}_{1s} + \Lambda - \xi_1 \]  \hspace{1cm} (11)

\[ N_s = n_{0s} + \tilde{N}_{1s} + \Lambda' + \xi_1 \]  \hspace{1cm} (12)

where

\[ \Lambda = \sum_{k=2}^{J} \sum_{i \in c_k} p_i a_{ki} d_{ki}; \quad \Lambda' = \sum_{k=2}^{J} \sum_{i \in c_k} p'_i a'_{ki} d_{ki}, \]  \hspace{1cm} (13)

and

\[ \xi_1 = n_{1s} - \tilde{N}_{1s} \geq 0 \]  \hspace{1cm} (14)

Using the expression of \( \Lambda' \), we will have:

\[ \Lambda' = \sum_{k=2}^{J} \sum_{i \in c_k} p'_i a'_{ki} \geq \sum_{k=2}^{J} \sum_{i \in c_k} \frac{1}{1 + \max_{j \in c_k} \left( \frac{p_j a_{jki}}{p'_j a'_{jki}} \right)} \hat{\Lambda} \]  \hspace{1cm} (15)
Further, we assume the important condition

\[
\max_{j \in c_k} \left( \frac{p_j a_{kj}}{p_j^i a_{kj}} \right) \leq \max_{j \in c_2} \left( \frac{p_j a_{2j}}{p_j^i a_{2j}} \right) \leq \max_{j \in c_1} \left( \frac{p_j a_{1j}}{p_j^i a_{1j}} \right), \quad \text{for all } k \geq 2. \quad (16)
\]

So we can write \( \Lambda' = \tilde{\Lambda} + \xi_2 \) and \( \xi_2 \geq 0 \). We also have:

\[
\Lambda = \sum_{k=2}^{J} \sum_{i \in c_k} \frac{p_i a_{ki}}{p_i a_{ki} + p_i^j a'_{ki}} = \sum_{k=2}^{J} \sum_{i \in c_k} \left( 1 - \frac{p_i^j a'_{ki}}{p_i a_{ki} + p_i^j a'_{ki}} \right)
\]

\[
= \sum_{k=2}^{J} \sum_{i \in c_k} \left( 1 - \frac{1}{1 + \max_{j \in c_k} \left( \frac{p_j a_{kj}}{p_j^i a_{kj}} \right)} \right) - \xi_2
\]

\[
= \sum_{k=2}^{J} \sum_{i \in c_k} \frac{\max_{j \in c_k} \left( \frac{p_j a_{kj}}{p_j^i a_{kj}} \right)}{1 + \max_{j \in c_k} \left( \frac{p_j a_{kj}}{p_j^i a_{kj}} \right)} - \xi_2
\]

\[
= \max_{j \in c_2} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right) \tilde{\Lambda} - \xi_2 - \xi_3
\]

where \( \xi_3 = \sum_{k=2}^{J} \sum_{i \in c_k} \frac{\max_{j \in c_1} \left( \frac{p_j a_{kj}}{p_j^i a_{kj}} \right) - \max_{j \in c_k} \left( \frac{p_j a_{kj}}{p_j^i a_{kj}} \right)}{1 + \max_{j \in c_k} \left( \frac{p_j a_{kj}}{p_j^i a_{kj}} \right)} \geq 0, \) according to Eq. (16).

With Eq. (17), Eq. (12) is equivalent to

\[
N_d = n_{od} + \max_{j \in c_1} \left( \frac{p_j a_{1j}}{p_j^j a_{1j}} \right) \tilde{N}_{1s} + \max_{j \in c_2} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right) \tilde{N}_{1s} \tilde{N}_{1s} - \xi_1 - \xi_2 - \xi_3
\]

\[
N_s = n_{0s} + \tilde{N}_{1s} + \tilde{\Lambda} + \tilde{\xi}_1 + \tilde{\xi}_2
\]

(18)

Given the Eqs. (11, 18), we can formulate \( \tilde{N}_{1s} \):

\[
\tilde{N}_{1s} = \frac{N_d - \max_{j \in c_2} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right) N_s + \max_{j \in c_2} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right) n_{0s} - n_{od} + \max_{j \in c_2} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right) \left( \xi_1 + \xi_2 \right) + \xi_1 + \xi_2 + \xi_3}{\max_{j \in c_1} \left( \frac{p_j a_{1j}}{p_j^j a_{1j}} \right) - \max_{j \in c_2} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right)}
\]

(19)

Since \( \xi_1, \xi_2, \) and \( \xi_3 \) are all non-negative, and \( \max_{j \in c_1} \left( \frac{p_j a_{1j}}{p_j^j a_{1j}} \right) - \max_{j \in c_2} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right) \geq 0 \) by Eq. (16), we now have

\[
\tilde{N}_{1s} \geq \frac{N_d - \max_{j \in c_2} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right) N_s + \max_{j \in c_2} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right) n_{0s} - n_{od}}{\max_{j \in c_1} \left( \frac{p_j a_{1j}}{p_j^j a_{1j}} \right) - \max_{j \in c_2} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right)}
\]

(20)

Therefore, we can now bound the fraction of single counts among all counts caused by the signal source

\[
\Delta_1 \geq \frac{\tilde{N}_{1s}}{N_s} \geq \frac{N_d - \max_{j \in c_2} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right) N_s + \max_{j \in c_2} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right) n_{0s} - n_{od}}{N_s \left( \max_{j \in c_1} \left( \frac{p_j a_{1j}}{p_j^j a_{1j}} \right) - \max_{j \in c_2} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right) \right)}
\]

\[
\geq \frac{N_d - \max_{j} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right) N_s + \max_{j} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right) n_{0s} - n_{od}}{N_s \left( \max_{j} \left( \frac{p_j a_{1j}}{p_j^j a_{1j}} \right) - \max_{j} \left( \frac{p_j a_{2j}}{p_j^j a_{2j}} \right) \right)}
\]

(21)
So:

$$\Delta_1 \geq \min_j \left( \frac{p_j a_{1j}}{p'_j a'_{1j}} \right) \Delta'_1$$

(22)

where \( \min_j = \min_{j \in C} \). In calculating the final key rate, we also need the relation between quantum bit error rate (QBER) for single-photon counts due to the decoy source \( e_{1d} \) and due to the signal source \( e_{1s} \). Suppose \( i \in c_1 \) and quantum bit flip probability is \( e_{1i} \). Then the total errors for single photon counts from each sources are:

$$e_{1d} = \frac{\sum_{i \in c_1} \frac{p_i a_{1i} e_{1i}}{p_i a_{1i} + p_i a'_{1i}}}{n_{1d}}$$

(23)

$$e_{1s} = \frac{\sum_{i \in c_1} \frac{p_i a'_i e_{1i}}{p_i a_{1i} + p_i a'_{1i}}}{n_{1s}}$$

(24)

Since \( n_{1s} = \sum_{i \in c_1} \frac{p_i a'_i}{p_i a_{1i} + p_i a'_{1i}} = \sum_{i \in c_1} \frac{p_i a_{1i}}{p_i a_{1i} + p_i a'_{1i}} \), we get:

$$n_{1s} \geq \frac{1}{\max_j \left( \frac{p_j a_{1j}}{p'_j a'_{1j}} \right)} n_{1d}$$

(25)

And there is:

$$\sum_{i \in c_1} \frac{p_i a'_i e_{1i}}{p_i a_{1i} + p_i a'_{1i}} \leq \frac{1}{\min_j \left( \frac{p_j a_{1j}}{p'_j a'_{1j}} \right)} \sum_{i \in c_1} \frac{p_i a_{1i} e_{1i}}{p_i a_{1i} + p_i a'_{1i}}$$

(26)

So:

$$e_{1s} \leq \frac{\max_j \left( \frac{p_j a_{1j}}{p'_j a'_{1j}} \right)}{\min_j \left( \frac{p_j a_{1j}}{p'_j a'_{1j}} \right)} e_{1d}$$

(27)

In the same reason, we can also give a lower bound of \( e_{1s} \). Finally we obtain

$$\frac{\min_j \left( \frac{p_j a_{1j}}{p'_j a'_{1j}} \right)}{\max_j \left( \frac{p_j a_{1j}}{p'_j a'_{1j}} \right)} e_{1d} \leq e_{1s} \leq \frac{\max_j \left( \frac{p_j a_{1j}}{p'_j a'_{1j}} \right)}{\min_j \left( \frac{p_j a_{1j}}{p'_j a'_{1j}} \right)} e_{1d}$$

(28)

If \( \frac{p_j a_{1j}}{p'_j a'_{1j}} \) and \( \frac{p_j a_{2j}}{p'_j a'_{2j}} \) are constant numbers for all \( j \in C \), then \( e_{1s} = e_{1d} \) and the last inequality in Eq. (21) is identical to Eq. (18) of Ref. [19], which is the formula of fraction of single-photon counts with a stable source. We conclude the following theorem:

**Theorem:** Decoy-state QKD with a fluctuating source can be used as if the source were stable if \( \frac{p_j a_{1j}}{p'_j a'_{1j}} \) and \( \frac{p_j a_{2j}}{p'_j a'_{2j}} \) are constant numbers for all \( j \in C \).
Interestingly, the condition in the theorem is not equivalent to Eq. (1), the elementary proposition given by Hwang [8]. Our theorem only depends on the fluctuation characterization of those pulses in set C, i.e., those pulses accompanied by a click of Bob’s detector, while Eq. (1) actually requests \( n_{kd}/N_{kd} = n_{1d}/N_{1d} \) therefore needs the fluctuation characterization of all pulses from Alice’s lab. Here \( N_{kd} \) and \( N_{ks} \) are number of k-photon pulses from decoy source and that from signal source, respectively. Given this fact, one can in principle construct specific cases where Eq. (1) does not hold while the condition in our theorem still holds. This shows that our Eq. (3) is indeed more fundamental and more general than Eq. (1).

C. Conclusion on AYKI protocol

The AYKI protocol uses a heralded source of:

\[
|\Psi_i\rangle_{AS} = \sum_{k=0}^{\infty} \sqrt{X_{ki}} |k\rangle_A |k\rangle_S
\]  

where \( X_{ki} = \mu_i^k (1 + \mu_i)^{-(k+1)} \). The heralded source state can be produced by, e.g., the parametric down conversion (PDC) which is pumped by strong light pulses whose intensity fluctuation can be as large as 20\%. In the protocol, Alice detects mode A and sends out mode S to Bob. Mode S is a decoy pulse when Alice’s detector clicks and a signal pulse when her detectors does not click. Suppose Alice’s detector has a detecting efficiency \( \eta_A \) and dark count rate \( d_A \). At any time \( i \), given the two mode state in Eq. (29), the probability that her detector clicks or not is

\[
p_i' = \frac{d_A + \mu_i \eta_A}{1 + \mu_i \eta_A} \\
p_i = \frac{1 - d_A}{1 + \mu_i \eta_A}
\]  

When the detector clicks or not, we obtain a signal state or a decoy state at mode S in the form of Eq. (2), and

\[
a_{ki} = \frac{1 + \mu_i \eta_A}{1 - d_A} X_{ki} (1 - \gamma_k) \\
\alpha'_{ki} = \frac{1 + \mu_i \eta_A}{d_A + \mu_i \eta_A} X_{ki} \gamma_k
\]  

and

\[
\gamma_k = 1 - (1 - d_A) (1 - \eta_A)^k
\]
We find
\[
\frac{p_i a_{ki}}{p_i' a'_{ki}} = \frac{1 - \gamma_k}{\gamma_n} = \frac{(1 - d_A)(1 - \eta_A)^k}{1 - (1 - d_A)(1 - \eta_A)^k}
\] (33)

They are independent on \(i\), hence source fluctuation does not change the final formula of the protocol by our theorem. Also, according to Eq. (21) we can write:
\[
n_{1s} = \tilde{N}_{1s} \geq N_d - \frac{1 - \gamma_2}{\gamma_2} N_s + \frac{1 - \gamma_2}{\gamma_2} n_{0s} - n_{0d}
\] (34)

Using the fact \(\frac{n_{0s}}{n_{0d}} = \frac{p_i' a'_{ki}}{p_i a_{ki}} = \frac{d_A}{1 - d_A}\) we have
\[
\Delta' \geq \frac{N_d - \frac{1 - \gamma_2}{\gamma_2} N_s - (1 - \frac{1 - \gamma_2}{\gamma_2} \frac{d_A}{1 - d_A}) n_{0d}}{N_s (\frac{1 - \gamma_1}{\gamma_1} - \frac{1 - \gamma_2}{\gamma_2})}
\] (35)

which is just the major formula in Ref. [12]. We have not used Eq. (1) in our proof, though the derivation given by AYKI [12] have assumed one constant intensity \(\mu\) and used the assumption of Eq. (1). Our proof concludes that the AYKI protocol actually works securely with whatever intensity fluctuation, though the key rate can be low if the source fluctuation is large, in which case one may observe poor values of \(N_s\) and \(N_d\).

III. IMPROVED FORMULA FOR 3-INTENSITY PROTOCOL

If we add a vacuum source to the 2-intensity protocol and uses vacuum source with probability \(p_{vi}\) at the \(i\)th time, we have a 3-intensity protocol where one can estimate number of vacuum counts \(n_{0s}, n_{0d}\) more precisely therefore improve the final key rate. Suppose the vacuum source caused \(N_0\) clicks. By similar derivation done in Ref. [19], we obtain
\[
n_{0d} \leq \frac{1}{p_0} \max_{j \in \epsilon_0} (p_j a_{0j}) \sum_{i \in \epsilon_0} p_0 d_{0i} \leq \frac{1}{p_0} \max_j (p_j a_{0j}) N_0.
\] (36)

A. Numerical simulation

In our major formula, Eq. (21), there are terms of \(\max_i\), this economic worst-case estimation can be significantly smaller than the normal worst-case of \(\frac{\max_i (p_i a_{ki})}{\min_i (p_i' a'_{ki})}\) estimation as proposed in Ref. [19], hence Eq. (21) can improve the key rate a lot. Consider the model that both decoy pulse and signal pulse are generated through attenuating a common father pulse at time \(i\). We set \(p_{vi} = p_0, p_i = p\) and \(p_i' = p'\) to be constants. The fluctuation of
the final pulse out of Alice’s lab consists of two parts: father pulse fluctuation and device (attenuator) parameter fluctuation. Suppose Alice wants to use intensity $\mu$, $\mu'$ for her decoy pulse and signal pulse. She wants to obtain them through attenuating the father pulse of intensity $F$ by setting her attenuator’s transmittance to be $\lambda_D = \frac{\mu}{F}$, $\lambda_S = \frac{\mu'}{F}$ for a decoy pulse or for a signal pulse. However, the actual case is that at any time $i$, the intensity of the father pulse is $F_i = F(1 + \delta_i)$, $\lambda_{Di} = \lambda_D(1 + \epsilon_{id})$ and $\lambda_{Si} = \lambda_S(1 + \epsilon_{is})$. We have the upper bounds of: $|\delta_i| \leq \delta$, $|\epsilon_{id}| \leq \epsilon_d$ and $|\epsilon_{is}| \leq \epsilon_s$. The actual intensity of the $i$th pulse out of Alice’s lab is

$$\text{decoy : } \mu_i = \mu(1 + \delta_i)(1 + \epsilon_{id})$$

$$\text{signal : } \mu_i' = \mu'(1 + \delta_i)(1 + \epsilon_{is})$$

$$\max_i \left( \frac{p_{ki}}{p_{ki}'} \right) = \frac{p}{p'} \left( \frac{\mu(1 + \epsilon_d)}{\mu'(1 - \epsilon_s)} \right)^k \exp\{(1 + \delta)[\mu'(1 - \epsilon_s) - \mu(1 + \epsilon_d)]\}$$

for $k \geq 1$

In a real experiment, only one pulse is prepared and sent out at any $i$th time. Values $\mu_i$ and $\mu_i'$ can be interpreted as the would-be values if Alice decided to produce a decoy pulse or signal pulse at the $i$th time, given a certain set-up. The bound of vacuum count in Eq.(35) is now $n_{0d} \leq \frac{n N_0}{p_0} e^{-\min_i(\mu_i)}$ and $n_{0s} \geq \frac{p' N_0}{p_0} e^{-\max_i(\mu_i')}$. Note that here we have taken the normal worst-case estimation only for the device fluctuation, while we have taken the economic worst-case estimation for the intensity fluctuation of the father pulse. Our result here also applies to a source state a little bit different from a coherent state: we just add very small new fluctuation terms to the parameters $a_{ki}$, $a_{ki}'$ in the states. If these terms are negligibly small, there effects to the final key rate is also negligible. Though there are also other methods[18, 20, 22] for decoy-state QKD with fluctuating source, they[18, 20, 22] only apply to the father pulse fluctuation, but not apply to the device fluctuation, as clearly pointed out in[20, 21]. As shown already, our method does not assume zero device fluctuation since it directly applies to the fluctuation of the final pulse out of Alice’s lab.

We use the experimental data for 50km given by done by Peng et al[16] QKD for numerical simulation. The results are shown in Fig.1, where we set $\epsilon_d = \epsilon_s = \epsilon$. We find that the fluctuation of the father pulse intensity changes the final key rate very slightly using Eq.(21) in this work in the calculation, while the device fluctuation still degrades the final key rate drastically. Our results here also apply to the Plug-and-Play protocol[25].
FIG. 1: Comparison of relative key rates to that of zero fluctuation. 

a: Relative key rates with father-pulse-intensity fluctuation at $\epsilon = 0$ and 2%. Line 1 and 2 are calculated with Eq. (21) of this work and Eq.(58) of Ref.[19], respectively.

b: Relative key rate with device fluctuation. 

b(left): Result calculated with Eq.(58) of Ref.[19]; b(right) Result calculated with Eq.[21]. Line 1 and 2 in b are for $\delta = 1\%, 6\%$, respectively.

IV. CONCLUDING REMARK AND DISCUSSIONS

In summary, we have presented a criteria for the secure decoy-state protocol with source fluctuation. The AYKI protocol satisfies the criteria. A well known advantage of AYKI protocol is that there is no need to make intensity switching. Given our proof here, AYKI protocol neither needs intensity switching nor needs source intensity monitoring. As the base of the conclusion, our general formulas here are efficient for other protocols, such as the 3-intensity protocol using coherent states. It should be interesting to include the finite size effects[3, 13, 26] in the future study.

Acknowledgement: We thank L. Yang for his help in the numerical simulation. This work was supported in part by the National Basic Research Program of China grant No. 2007CB907900 and 2007CB807901, NSFC grant No. 60725416 and China Hi-Tech program grant No. 2006AA01Z420.

[1] C.H. Bennett and G. Brassard, in Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing (IEEE, New York, 1984), pp. 175-179.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002); N. Gisin
and R. Thew, Nature Photonics, 1, 165 (2006); M. Dusek, N. Lütkenhaus, M. Hendrych, in Progress in Optics VVVX, edited by E. Wolf (Elsevier, 2006); V. Scarani, H. Bechmann-Pasquonnucc, N.J. Cerf, M. Dusek, N. Lütkenhaus, and M Peev, Rev. Mod. Phys. 81, 1301 (2009).

[3] H. Inamori, N. Lütkenhaus, D. Mayers, European Physical Journal D, 41, 599 (2007), which appeared in the arXiv as quant-ph/0107017

[4] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A 51, 1863 (1995); H.P. Yuen, Quantum Semiclassic. Opt. 8, 939 (1996).

[5] G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sanders, Phys. Rev. Lett. 85, 1330 (2000); N. Lütkenhaus, Phys. Rev. A 61, 052304 (2000); N. Lütkenhaus and M. Jahma, New J. Phys. 4, 44 (2002).

[6] D. Gottesman, H.K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. 4, 325 (2004).

[7] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Physics Reports 448, 1(2007)

[8] W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).

[9] X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005); X.-B. Wang, Phys. Rev. A 72, 012322 (2005).

[10] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005); X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A 72, 012326 (2005).

[11] J.W. Harrington et al., quant-ph/0503002

[12] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev.Lett. 99, 180503 (2007).

[13] M. Hayashi, Phys. Rev. A 74, 022306 (2008); ibid 76, 012329 (2007).

[14] V. Scarani, A. Acin, G. Ribordy, N. Gisin, Phys. Rev. Lett. 92, 057901 (2004); C. Branciard, N. Gisin, B. Kraus, V. Scarani, Phys. Rev. A 72, 032301 (2005).

[15] M. Koashi, Phys. Rev. Lett., 93, 120501(2004); K. Tamaki, N. Lükenhaus, M. Koashi, J. Batsuwantudawe, quant-ph/0612082

[16] D. Rosenberg em et al., Phys. Rev. Lett. 98, 010503 (2007); T. Schmitt-Manderbach et al., Phys. Rev. Lett. 98, 010504 (2007); Cheng-Zhi Peng et al. Phys. Rev. Lett. 98, 010505 (2007); Z.-L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. 90, 011118 (2007); Y. Zhao, B. Qi, X. Ma, H.-K. Lo and L. Qian, Phys. Rev. Lett. 96, 070502 (2006); Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, in Proceedings of IEEE International Symposium on Information Theory, Seattle, 2006, pp. 2094–2098 (IEEE, New York).

[17] X.-B. Wang, Phys. Rev. A75, 012301(2007)
[18] X.-B. Wang, C.-Z. Peng and J.-W. Pan, Appl. Phys. Let. 90, 031110 (2007).

[19] X.-B. Wang, C.-Z. Peng et al. Phys. Rev. A 77, 042311 (2008).

[20] Y. Zhao et al, Phys. Rev. A 77, 052327 (2008).

[21] X.-B. Wang, L. Yang, C.-Z. Peng and J.-W. Pan, New J. Phys. 11, 075006 (2009).

[22] Y. Zhao, B. Qi, H.-K. Lo, and Q. Li, New J. Phys. 12, 023024 (2010).

[23] F.X. Xu, Y. Zhang, Z. Zhou, W. Chen, Z. F. Han, and G. C. Guo, Phys. Rev. A, 80, 062309 (2009).

[24] X. Peng, H. Jiang, B.J. Xu, X.F. Ma, and H. Guo, Opt. Lett., 33, 2077 (2008).

[25] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A 73, 022320 (2006).

[26] Raymond Y. Q. Cai and V. Scarani, New J. Phys., 11, 11, 045024 (2009).