Decoy-state quantum key distribution with both source errors and statistical fluctuations

Xiang-Bin Wang\textsuperscript{1,2,6}, Lin Yang\textsuperscript{1,3}, Cheng-Zhi Peng\textsuperscript{1,4} and Jian-Wei Pan\textsuperscript{1,4,5}

\textsuperscript{1}Department of Physics, Tsinghua University, Beijing 100084, People’s Republic of China
\textsuperscript{2}Tsinghua National Laboratory for Information Science and Technology, Beijing 100084, People’s Republic of China
\textsuperscript{3}Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, People’s Republic of China
\textsuperscript{4}Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, People’s Republic of China
\textsuperscript{5}Physikalisches Institut, Universität Heidelberg, Philosophenweg 12, 69120 Heidelberg, Germany
E-mail: xbwang@mail.tsinghua.edu.cn

New Journal of Physics \textbf{11} (2009) 075006 (17pp)
Received 26 February 2009
Published 15 July 2009
Online at \url{http://www.njp.org/}
doi:10.1088/1367-2630/11/7/075006

\textbf{Abstract.} We show how to calculate the fraction of single-photon counts of the 3-intensity decoy-state quantum cryptography faithfully with both statistical fluctuations and source errors. Our results rely only on the bound values of a few parameters of the states of pulses.

\textsuperscript{6}Author to whom any correspondence should be addressed.
1. Introduction

Quantum key distribution (QKD) [1]–[7] has now been extensively studied both theoretically and experimentally. In practice, if one uses an imperfect single-photon source with a lossy channel, the security is undermined by the photon-number-splitting attack [8, 9]. Fortunately, this can be managed by a number of methods [4], [10]–[20]. In particular, the so-called ILM-GLLP proof [4, 5] has shown that if we know the upper bound of the fraction of multi-photon counts (or equivalently, the lower bound of single-photon counts) among all raw bits, we still have a way to distill the secure final key. Verifying such a bound is strongly nontrivial. The so-called decoy-state method [10]–[14] is to find such bounds, say, among all those clicks at Bob’s side, at least how many of them are due to the single-photon pulses from Alice.

The main idea of the decoy-state method is to change intensities randomly among different values in sending out each pulse. Equivalently, we can regard pulses of different intensities as pulses from different sources. For example, in a 3-intensity protocol [12], Alice has three sources, source $Y_0$ (vacuum source) that is supposed to only produce vacuum, source $Y$ (decoy source) that is supposed to only produce state

$$\rho = \sum_{k=0}^{J} a_k |k\rangle \langle k|$$

only, and source $Y'$ (signal source) that is supposed to only produce state

$$\rho' = \sum_{k=0}^{J} a_k' |k\rangle \langle k|,$$

where $|k\rangle$ is the $k$-photon Fock state and $a_k \geq 0$, $a_k' \geq 0$ for all $k$, $\sum a_k = \sum a_k' = 1$. Here $J$ can be either finite or infinite. Given a coherent-state source or a heralded single-photon source from the parametric down conversion, $J = \infty$. 

New Journal of Physics 11 (2009) 075006 (http://www.njp.org/)
The fundamental formula in the decoy-state method as first proposed by Hwang [11] is that the counting rates (yields) of pulses of the same photon-number states must be equal to each other even if they are from different sources, i.e.

\[ s_k = s'_k, \]  

(3)

where \( s_k \) and \( s'_k \) are the counting rate of \( k \)-photon pulses from the decoy source and the counting rate of \( k \)-photon pulses from the signal source, respectively. This is because of the obvious fact that those \( k \)-photon pulses from different sources are actually randomly mixed; therefore they are random samples of each other if sources \( Y_0, Y \) and \( Y' \) are perfectly stable, i.e. they always produce a state precisely as the assumed one. Given equation (3), one can list simultaneous equations [12] for \( s_k \)-based equations (1) and (2), and then find the lower bound of \( s_1 (s'_1) \), which indicates the lower bound of single-photon counts of the decoy source and signal source.

Given this, one can calculate the final key rate of each source by the well-known result of ILM-GLLP [4, 5]. For example, the asymptotic final key rate for the signal source can be calculated by

\[ R_s = \Delta'_1 [1 - H(t_1)] - H(t), \]  

(4)

where \( t_1, t \) are the quantum bit error rate (QBER) for single-photon counts of the signal source and the QBER for all counts of the signal pulses from the signal source. \( \Delta'_1 \) is the lower bound of the fraction of counts due to single-photon pulses from the signal source. Moreover, the non-asymptotic unconditional secure key rate in a finite-size QKD has been extensively studied recently, first in [4] and then further in [6, 7].

Recently, a number of QKD experiments using the decoy-state method have been done [21]–[25]. However, the story is not completed here because the existing decoy-state theory does not entirely cover the real experimental conditions in practice. No source in real life can be perfectly stable. One important problem is the effect of source errors. Suppose in a protocol Alice sends out \( M \) pulses one by one. The actually produced state at any time \( i \) can differ from the assumed state that she wants. We call this discrepancy source error. Say, at any time \( i \), Alice wants to prepare a state

\[ \rho_i = \sum_{k=0}^{J} f_k |k\rangle \langle k| \]  

(5)

for Bob, but the source actually prepares a slightly different state

\[ \tilde{\rho}_i = \sum_{k=0}^{J} f_{ki} |k\rangle \langle k| \]  

(6)

in the Fock space. We call such \( f_{ki} - f_k \) source error, state error or parameter fluctuation. Most generally, the error \( f_{ki} - f_k \) is not random for different \( i \). In practice, one of the major causes of source error is intensity fluctuation. Therefore we often use the term intensity fluctuation for source errors. But our result here is not limited to the intensity fluctuation only. Here we consider a more general case in which the parameters in the state fluctuate. Therefore we still use the term source error instead of intensity fluctuation.

If the source error is random, we can simply assume a perfectly stable source always emitting the averaged state [14, 26] of all pulses from a certain source. As shown in [26], we have to take a feed-forward control to each individual pulse in order to guarantee the randomness...
of source errors. If we use coherent light only, and if we have a stable two-value attenuator, we can use the method in [27] to manage any intensity fluctuations.

If we do not assume any conditions above, the issue needs to be studied more carefully. A very tricky point here is that the elementary assumption of equation (3) for the decoy-state method with stable sources is in general incorrect, if the state errors are not random. As we have shown explicitly [10, 28], there are cases that Eve may know the source errors and she can violate equation (3) by producing an instantaneous transmittance channel dependent on the errors. Therefore, we must seek a solution to the new problem.

Very recently [28], a general theory for decoy-state QKD with source errors is presented. By the method [28], we do not have to change anything in the existing setup. The only thing we need is the bound values of a few parameters in the states from each source. Besides [28], the problem is also studied [29] from another viewpoint for the Plug-and-Play protocol. There [29], Alice receives a pulse, attenuates it and sends it out for Bob. Eve controls both the incident pulse and the outcome pulse. Alice’s transmittance $\gamma$ in doing attenuation can be either $\gamma^b$ or $\gamma^s$, depending on whether she wants to prepare a decoy pulse or a signal pulse. Similar to [27], [29] also assumes that Alice can do the two-value attenuation exactly. The fundamental formula assumed there [29] is

$$ Y^{D}_{m,n} = Y^{S}_{m,n}, $$

where $Y^{D}_{m,n}$ ($Y^{S}_{m,n}$) is the counting rate of a decoy (signal) pulse, which contains $m$ photons when flying into Alice’s lab and contains $n$ photons when flying away from Alice’s lab, after Alice’s attenuation. As was pointed out by the authors of [29], the effects of the internal fluctuation of Alice’s lab were not considered there and also the validity of elementary equation $Y^{D}_{m,n} = Y^{S}_{m,n}$ was not studied. Actually, as shown in the appendix of this work, the elementary equation does not always hold if there are fluctuations to Alice’s attenuation.

In this paper, we study the effects of both source errors and classical statistical fluctuations. The existing works [28, 29] have not included the effect of statistical fluctuations in calculating the final key rate, though the effect can be included in principle. Our earlier work assumes zero error for vacuum source $Y_0$; here we shall assume errors in this source, besides errors in source $Y$ and source $Y'$. Similar to the results in [28], the results presented here only need the bound values of a few parameters in the states of different sources. In particular, in deriving the fraction of single-photon counts we do not use any unproven assumption and we do not need to worry about the internal fluctuation of Alice’s device, since our method only needs the bound values of a few parameters in the source state. We do not need to presume any specific distribution for our states. In our study in this work, classical statistical fluctuation is considered by estimating the observed values from the asymptotic values with a fixed standard deviation. We shall start with a protocol with one-way quantum communication only. But as we point out at the end of this paper, our method obviously also applies to a Plug-and-Play protocol.

The present paper is arranged as followings. After the introduction above, we present our method with some important mathematical relations in section 2. We then present our main results in section 3: the asymptotic and non-asymptotic formulae for the fraction of single-photon counts of the three-intensity protocol with errors in states of all 3 sources.

As was discussed in the end of the conclusion section of [29]: ‘The security of practical QKD is a serious issue. It is very important to implement QKD system based on tested assumptions. There are still several crucial imperfections that are not analyzed in this paper. For example . . . How can we analyze the fluctuation of internal transmittance $\lambda$? How can we test the key assumptions in our analysis, $Y^{S}_{m,n} = Y^{D}_{m,n}$ . . .’.
remarks on the source errors are addressed in section 4. The paper ends with a concluding remark.

2. Our method

We assume that Alice sends $M$ pulses to Bob one by one in the protocol. Each pulse sent out by Alice is randomly chosen from one of the three sources $Y_0$, $Y$ and $Y'$ with constant probability $p_0$, $p$ and $p'$, respectively. Each source has errors. Clearly, $pM$, $p'M$ and $p_0M$ are just the number of decoy pulses, the number of signal pulses and the number of pulses from the vacuum source, respectively. We assume knowing the bounds of parameters in the states of each source.

Our goal is to find the lower bound of the fraction of counts caused by those single-photon pulses for both the signal source and the decoy source. The following quantities are directly observed in the protocol; therefore we regard them as known parameters: $N_d$, the number of counts caused by the decoy source, $N_s$, the number of counts caused by the signal source, and $N_0$, the number of counts caused by the vacuum source, $Y_0$. For our goal, we only need to formulate the number of counts caused by those single-photon pulses from each source in terms of the known quantities $N_0$, $N_d$, $N_s$ and $p_0$, $p$, $p'$ and the bound values of those parameters of states in each source.

2.1. Virtual protocol

For clarity, we first consider a virtual protocol. Suppose Alice sends $M$ pulses to Bob in the whole protocol. At any time $i$ ($i \in [1, M]$), each source produces a pulse. The states of the pulses from sources $Y_0$, $Y$, $Y'$ are

$$\rho_0 = \sum_{k=0}^{j} b_{ki} |k\rangle \langle k|,$$

$$\rho_i = \sum_{k=0}^{j} a_{ki} |k\rangle \langle k|,$$

$$\rho'_i = \sum_{k=0}^{j} a'_{ki} |k\rangle \langle k|.$$

Here $b_{0i}$ is slightly smaller than 1, and we assume that $b'_{0i}$, the lower bound of all $b_{0i}$, is known in the protocol; $\rho_i$ and $\rho'_i$ are slightly different from $\rho$ and $\rho'$ of equations (1) and (2), which are the assumed states in the perfect protocol where there is no source error. At any time $i$, only one pulse is selected and sent out for Bob. The probability of selecting the $i$th pulse source $Y_0$, $Y$ or $Y'$ is constantly $p_0$, $p$ and $p'$ for any $i$. The unselected two pulses at each time will be discarded. After Bob has completed all measurements to the incident pulses, Alice checks the record about which pulse is selected at each time, i.e. which time has used which source. Obviously, Alice can decide which source is to be used at each time in the very beginning. This is just then the real protocol of the decoy-state method.

As shown below, based on this virtual protocol, we can formulate the number of counts from each source and therefore find the lower bound of the number of single-photon counts. The result also holds for the real protocol where Alice decides to use which sources at the $i$th time in the very beginning.
2.2. Some definitions

**Definition 1.** In the protocol, Alice sends Bob $M$ pulses, one by one. In response to Alice, Bob observes his detector $M$ 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 only need Bob’s detector clicks in Bob’s $i$th observation.

Given the source state in equations (8) and (9), any $i$th pulse sent out by Alice must be in a photon number state. To anyone outside Alice’s lab, it looks as if Alice only sends a photon number state at each single shot: sometimes it is a vacuum, sometimes it is a single-photon pulse, sometimes it is a $k$-photon pulse, and so on. We shall make use of this fact that any individual pulse is in one Fock state.

**Definition 2.** Set $C$ and $c_k$: Set $C$ contains any pulse that has caused a count; set $c_k$ contains any $k$-photon pulse that has caused a count. Mathematically speaking, 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 $C = \{i | i = 2, 3, 5, 6, 9, 10, \ldots\}; c_0 = \{i | i = 2, 5, 10, \ldots\}; c_1 = \{i | i = 3, 6, 9, \ldots\}$.

Clearly, $C = c_0 \cup c_1 \cup c_2 \ldots$, and every pulse in set $C$ has caused a count.

**Definition 3.** We use superscripts $U, L$ for the upper bound and lower bound of a certain parameter. In particular, given any $k \geq 0$ in equations (7)–(9), we denote $x^{L}_{ki}, x^{U}_{ki}$ for the minimum value and maximum value of $\{x_{ki} | i \in c_k\}$, and $x = b, a, a'$. We assume these bound values are known in the protocol.

2.3. Some important relations and facts

If the $i$th pulse is an element of $c_k$, the probability that it is from $Y_0$, $Y$ or $Y'$ is

\[
\mathcal{P}_{vi|k} = \frac{p_0 b_{ki}}{p_0 b_{ki} + p a_{ki} + p' a'_{ki}},
\]

\[
\mathcal{P}_{di|k} = \frac{p a_{ki}}{p_0 b_{ki} + p a_{ki} + p' a'_{ki}},
\]

\[
\mathcal{P}_{si|k} = \frac{p' a'_{ki}}{p_0 b_{ki} + p a_{ki} + p' a'_{ki}}.
\]

We want to formulate the numbers of $k$-photon counts caused by each source. Given the definition of the set $c_k$, this is equivalent to asking how many pulses in set $c_k$ come from each source. If the $i$th pulse contains $k$ photons, it can come from any of the three sources, $Y_0, Y$ or $Y'$. According to equations (7)–(9), if the $i$th pulse contains $k$-photons, the probability that it comes from source $Y_0$ is

\[
\mathcal{P}_{vi|k} = \frac{b_{ki} p_0}{p_0 b_{ki} + p a_{ki} + p' a'_{ki}}.
\]
Or, equivalently,

\[ n_{k0} = \sum_{i \in c_k} P_{vij}. \]

Given a finite number of pulses and counts, this equation should be replaced by the expectation-value equation as

\[ \langle N_0 \rangle = \sum_{k=0}^{j} \sum_{i \in c_k} P_{vij} \].

(12)

This is the expected number of counts caused by source \( Y_0 \), since every pulse in \( \{c_k\} \) has caused a count. Therefore we can formulate the expected value of the number of counts caused by source \( Y_0 \) by

\[ \langle N_0 \rangle = \sum_{k=0}^{j} \sum_{i \in c_k} b_{ki} p_0 d_{ki} = \langle N_0^* \rangle + \sum_{k=1}^{j} \sum_{i \in c_k} b_{ki} p_0 d_{ki}. \]

(13)

Here

\[ d_{ki} = \frac{1}{p_0 b_{ki} + p a_{ki} + p' a'_{ki}}. \]

(14)

\( N_0 \) is the number of counts due to pulses from source \( Y_0 \) and \( N_0^* = p_0 \sum_{i \in c_0} b_{0i} d_{0i} \) is the number of counts due to those vacuum pulses from source \( Y_0 \). Similarly, if the \( i \)th pulse contains \( k \) photons, it has a probability \( P_{d|ki} = \frac{pa_{ki}}{p_0 b_{ki} + pa_{ki} + p' a'_{ki}} \) to be from the decoy source, and a probability of \( P_{s|ki} = \frac{p' a'_{ki}}{p_0 b_{ki} + pa_{ki} + p' a'_{ki}} \) to be from the signal source. Therefore we have

\[ \langle n_{k0} \rangle = \sum_{i \in c_k} P_{d|ki} = \sum_{i \in c_k} p a_{ki} d_{ki} \]

(15)

for the expected number of counts caused by those \( k \)-photon pulses from the decoy source, and

\[ \langle n'_{k0} \rangle = \sum_{i \in c_k} P_{s|ki} = \sum_{i \in c_k} p' a'_{ki} d_{ki} \]

(16)

for the expected number of counts caused by those \( k \)-photon pulses from the signal source. Therefore, besides equation (13) we also have the following two equations for \( \langle N_d \rangle \) and \( \langle N_s \rangle \) as the expected values of the number of counts due to decoy pulses and signal pulses:

\[ \langle N_d \rangle = \sum_{k=0}^{j} \sum_{i \in c_k} P_{d|ki} = p \sum_{k=0}^{j} \sum_{i \in c_k} a_{ki} d_{ki}, \]

(17)

\[ \langle N_s \rangle = \sum_{k=0}^{j} \sum_{i \in c_k} P_{s|ki} = p' \sum_{k=0}^{j} \sum_{i \in c_k} a'_{ki} d_{ki}. \]

(18)

Here we have used equations (15) and (16).

For simplicity, we define

\[ D_k = \sum_{i \in c_k} d_{ki} = \sum_{i \in c_k} \frac{1}{p_0 b_{ki} + p a_{ki} + p' a'_{ki}}. \]

(19)
Recalling equations (16) and (15), \( \langle n'_0 \rangle \) and \( \langle n_{0d} \rangle \) are the expected numbers of pulses from the decoy source and signal source in set \( c_0 \).

Based on the formulae and definitions above, we find the following important facts.

**Fact 1:**

\[
p a_0^U D_0 \geq \langle n_{0d} \rangle \geq p a_0^L D_0; \quad p' a_0'^U D_0 \geq \langle n'_0 \rangle \geq p' a_0'^L D_0.
\]  

(20)

This is directly deduced from equations (15) and (16).

**Fact 2:**

\[
\frac{\langle N_0 \rangle}{b_0^L p_0} D_0 \geq \langle n_{0d} \rangle \geq \frac{a_1^L}{p_0 [a_1^L - a_0^L (1 - b_0^L)]} \left( \langle N_0 \rangle - \frac{p_0 (1 - b_0^L)}{p a_1^L} \langle N_d \rangle \right).
\]  

(21)

**Proof:** Obviously,

\[
D_0 \leq \frac{\langle N_0 \rangle}{b_0^L p_0}.
\]  

(22)

On the other hand, since any \( b_{0i} \leq 1 \),

\[
p_0 D_0 \geq \langle N_0 \rangle - p_0 \sum_{k=1}^{J} \sum_{i \in c_k} b_{ki} d_{ki} \geq \langle N_0 \rangle - p_0 \sum_{k=1}^{J} b_k^U D_k.
\]  

(23)

To lower bound \( D_0 \), we only need upper bound \( p_0 \sum_{k=1}^{J} b_k^U D_k \). By equation (17) we know

\[
p \sum_{k=1}^{J} a_k^L D_k \leq \langle N_d \rangle - \langle n_{0d} \rangle,
\]  

(24)

which is equivalent to saying that

\[
p_0 b_1^U \sum_{k=1}^{J} a_k^L D_k \leq \frac{p_0 b_1^U}{p a_1^L} \left( \langle N_d \rangle - \langle n_{0d} \rangle \right).
\]  

(25)

We assume

\[
a_k^L \geq \frac{a_1^L}{b_k^U}.
\]  

(26)

This condition can obviously hold if each pulse of source \( Y_0 \) is in an extremely weak coherent state. These conditions mean that

\[
p_0 \sum_{k=1}^{J} b_k^U D_k \leq \frac{p_0 b_1^U}{p a_1^L} \left( p \sum_{k=1}^{J} a_k^L D_k \right).
\]  

(27)

Therefore, based on equations (23) and (25) we have

\[
p_0 D_0 \geq \langle N_0 \rangle - \frac{p_0 b_1^U}{p a_1^L} \left( \langle N_d \rangle - \langle n_{0d} \rangle \right) \geq \langle N_0 \rangle - \frac{p_0 (1 - b_0^L)}{p a_1^L} \left( \langle N_d \rangle - \langle n_{0d} \rangle \right).
\]  

(28)

Combining fact 1 with equation (28), we obtain the following important formula:

\[
D_0 \geq \frac{a_1^L}{p_0 [a_1^L - a_0^L (1 - b_0^L)]} \left( \langle N_0 \rangle - \frac{p_0 (1 - b_0^L)}{p a_1^L} \langle N_d \rangle \right).
\]  

(29)

This completes the proof of fact 2.
Fact 3:

\[ D_1 \geq D_1^L = \frac{a_2^L \langle N_d \rangle / p - a_2^U \langle N_s \rangle / p' - (a_2^L a_1^U - a_2^U a_1^L) D_0}{a_1^U a_2^L - a_1^L a_2^U}. \]  \hspace{1cm} (30)

**Proof:** The startpoint of our proof is equations (17) and (18), which can be rewritten as

\[ \langle N_d \rangle = \langle n_{0d} \rangle + p a_1^U D_1 + p \Lambda - \xi_1, \]  \hspace{1cm} (31)

\[ \langle N_s \rangle = \langle n_{0s} \rangle + p' a_1^L D_1 + p' \Lambda' + \xi_2, \]  \hspace{1cm} (32)

where

\[ \Lambda = \sum_{k=2}^{J} a_k^U \sum_{i \in c_i} d_{ki} \quad \Lambda' = \sum_{k=2}^{J} a_k^L \sum_{i \in c_i} d_{ki}, \]  \hspace{1cm} (33)

and

\[ \xi_1 = p \left[ a_1^U D_1 + \Lambda - \left( \sum_{i \in c_1} a_{1i} d_{1i} + \sum_{k=2}^{J} \sum_{i \in c_k} a_{ki} d_{ki} \right) \right] \geq 0, \]

\[ \xi_2 = p' \left[ \sum_{i \in c_1} a_{1i} d_{1i} + \sum_{k=2}^{J} \sum_{i \in c_k} a_{ki} d_{ki} - (a_1^L D_1 + \Lambda') \right] \geq 0. \]

According to the definition of \( \Lambda \) and \( \Lambda' \), we also have

\[ \Lambda' = \frac{a_2^L}{a_2^U} \Lambda + \xi_3 \]  \hspace{1cm} (34)

and

\[ \xi_3 = \Lambda' - \frac{a_1^L}{a_1^U} \Lambda. \]  \hspace{1cm} (35)

Further, we assume the important condition

\[ \frac{a_k^L}{a_k^U} \geq \frac{a_2^L}{a_2^U} \geq \frac{a_1^L}{a_1^U}, \]  \hspace{1cm} (36)

for all \( k \geq 2 \).

The first inequality above leads to

\[ \xi_3 \geq 0, \]  \hspace{1cm} (37)

as one may easily prove. With equation (34), equation (32) is converted to

\[ \langle N_s \rangle = \langle n_{0s} \rangle + p' a_1^L D_1 + p' \frac{a_2^L}{a_2^U} \Lambda + \xi_2 + p' \xi_3. \]  \hspace{1cm} (38)

Given equations (31) and (38), we can formulate \( D_1 \):

\[ D_1 = \frac{a_2^L \langle N_d \rangle / p - a_2^U \langle N_s \rangle / p' - a_2^L \langle n_{0d} \rangle / p + a_2^U \langle n_{0s} \rangle / p' + a_2^L \xi_1 / p + a_2^U (\xi_2 + p' \xi_3) / p'}{a_1^U a_2^L - a_1^L a_2^U}. \]  \hspace{1cm} (39)
Since $\xi_1$, $\xi_2$ and $\xi_3$ are all non-negative, and $a_1^L a_2^L - a_1^L a_2^U \geq 0$ by the second inequality of equation (36), we now have

$$D_1 = \sum_{i \in I} d_i \geq \frac{a_1^L (N_d) / p - a_2^U (N_s)}{a_1^U a_2^L - a_1^L a_2^U} \cdot a_1^L \frac{a_2^L (N_d) / p - a_2^U (N_s)}{a_1^U a_2^L - a_1^L a_2^U} \geq \frac{a_1^L (N_d) / p - a_2^U (N_s) / p - (a_1^L a_0^U - a_2^L a_0^U) D_0}{a_1^U a_2^L - a_1^L a_2^U} = D_1^L.$$  \hspace{1cm} (40)

Here we have used fact 1 for the bound values of $\langle n_{0d} \rangle$, $\langle n_{0b} \rangle$. To minimize $D_1$, we have replaced $\langle n_{0d} \rangle$ by its upper bound and $\langle n_{0b} \rangle$ by its lower bound as given in fact 1. This completes the proof of fact 3.

\[ \square \]

3. Main results

3.1. Asymptotic result

Given fact 3, the minimum value of the number of counts caused by single-photon pulses from the signal source (or the decoy source) is simply

$$\langle n_{1s} \rangle^L = p' a_1^L D_1 \leq \langle n_{1s} \rangle \quad \text{(or } \langle n_{1d} \rangle^L = p a_1^L D_1 \leq \langle n_{1d} \rangle \text{)}).$$  \hspace{1cm} (41)

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

$$\Delta_1^L \geq \frac{p' a_1^L D_1^L}{\langle N_s \rangle} = \frac{a_1^L (a_2^L (N_d) / p - a_2^U (N_s) / p) - p' (a_1^L a_0^U - a_2^L a_0^U) D_0}{\langle N_s \rangle (a_1^L a_2^L - a_1^L a_2^U)}.$$  \hspace{1cm} (42)

Here the range of $D_0$ is given by fact 2 in the previous subsection. We do not have to replace $D_0$ by its largest possible value to obtain the smallest possible $\Delta_1^L$ at this moment. Instead, we shall do numerical calculation by equation (4) with all possible values of $D_0$ in the range given by fact 2 and find the worst-case result directly to the key rate. Defining $S' = \frac{\langle N_s \rangle}{p M}$ as the counting rate of the signal source, $S = \frac{\langle N_s \rangle}{p M}$ as the counting rate of the decoy source, $S_0 = \frac{\langle N_s \rangle}{p M}$ as the counting rate of source $Y_0$ and $\hat{M}$ as the total number of pulses as defined earlier, we can write the right-hand side of the inequality in terms of counting rates:

$$\Delta_1^L \geq \frac{a_1^L \left[ a_2^L S - a_2^U S' - (a_1^L a_0^U - a_2^L a_0^U) S_0 / b_0^L \right]}{S' (a_1^L a_2^L - a_1^L a_2^U)}.$$  \hspace{1cm} (43)

Similarly, we also have

$$\Delta_1 \geq \frac{a_1^L \left[ a_2^L S - a_2^U S' - (a_2^L a_0^U - a_2^L a_0^L) S_0 / b_0^L \right]}{S (a_1^L a_2^L - a_1^L a_2^U)},$$  \hspace{1cm} (44)

for the minimum value of the fraction of single-photon counts for the decoy source.

Equations (42)–(44) and conditions of equations (26) and (36) are the asymptotic results of this work.

New Journal of Physics 11 (2009) 075006 (http://www.njp.org/)
3.2. Non-asymptotic results

Strictly speaking, equations (41) and (30) cannot be used in a real experiment where the number of pulses are always finite. Therefore, in any real experiment we have to consider the effect of statistical fluctuation besides the effect of source errors.

Firstly, \( \langle n'_1 \rangle_L = p' a'_1 D_1 \geq p' a'_1 D_1 \) in the formulae is the lower bound of the expected number of single-photon counts of the signal source, but we actually need the lower bound of \( n'_1 \), the (deduced) observed value (i.e. the true value) of the number of single-photon counts of the signal source in a certain experiment. Of course, given the expectation value, \( \langle n'_1 \rangle_L \), one can deduce the lower bound \( n'_1 \) of the experimental value \( n'_1 \) by classical statistics:

\[
| n'_1 \rangle_L = | n'_1 \rangle - \delta_1. \tag{45}
\]

To be sure that this bound is correct with a probability exponential close to 1, we need to set \( \delta_1 \) considerably large, e.g.

\[
\delta_1 = 10 \sqrt{| n'_1 \rangle}. \tag{46}
\]

Here ten standard deviations is chosen simply for convenience rather than an exact cut-off point. As shown in [12], the probability that the statistical fluctuation exceeds this range is exponentially close to 0.

Secondly, on the right-hand side of equation (30), there are many parameters of expectation values such as \( \langle N_d \rangle, \langle N_s \rangle, \langle n'_0 \rangle, \langle n''_0 \rangle \), which are not observed values in one specific experiment. We need to replace these parameters by experimentally observed quantities to make the formula useful. Again, this can be done by using classical statistics. This is to say, we need to consider the largest possible difference between the expectation values and the observed values due to statistic fluctuations.

For clarity, we shall use \( \langle \zeta \rangle \) for the statistical expectation value of observable \( \hat{\zeta} \) and \( \zeta \) for the true value or the observed value in the experiment. For example, we shall use \( \langle n_{1d} \rangle \) for the expectation value of the number of counts at Bob’s side due to the single-photon pulses from the decoy source at Alice’s side. We shall also use the superscript \( U \) or \( L \) to indicate the maximum value or minimum value of a certain variable. With the following condition

\[
P_{vi|k} + P_{di|k} + P_{si|k} = 1, \quad \text{if } i \in c_k \tag{47}
\]

for any \( k \), we can now start to derive our non-asymptotic result. By classical statistics we know that there exists a real number \( \delta_d \) satisfying

\[
N_d = \langle N_d \rangle + \delta_d \tag{48}
\]

with a probability exponentially close to 1 if we set

\[
| \delta_d | \leq \delta^U_d = 10 \sqrt{\langle N_d \rangle} \approx 10 \sqrt{N_d}. \tag{49}
\]

This indicates that

\[
\langle N_d \rangle = N_d - \delta_d \tag{50}
\]

with a probability exponentially close to 1 that \( \delta_d \) is in the range given by equation (49). Also, there exists a real number \( \delta_0 \) satisfying

\[
\langle N_0 \rangle = N_0 - \delta_0 \tag{51}
\]

and \( | \delta_0 | \leq 10 \sqrt{N_0} \).

New Journal of Physics 11 (2009) 075006 (http://www.njp.org/)
In our problem, due to the constraint given in equation (47), the fluctuations of each variable are not independent. This can help us not to overestimate the effects of the fluctuations too much. Equation (47) immediately leads to the following identity:

\[ \langle N_s \rangle + \langle N_d \rangle + \langle N_0 \rangle = N_s + N_d + N_0. \]  

(52)

This is to say, the total population in set C is fixed, but there could be fluctuation in the population distribution over sources \( Y_0, Y \) and \( Y' \). Equation (52), together with equations (50) and (51), leads to

\[ \langle N_s \rangle = N_s - \delta_d - \delta_0. \]  

(53)

We use

\[ n'_{1s} \geq \tilde{n}'_{1s} = \langle n'_{1s} \rangle - 10\sqrt{\langle n_{1s} \rangle}. \]  

(54)

This is the inequality for the experimental lower bound of the number of single-photon counts from decoy pulses, where

\[ \langle n'_{1s} \rangle \geq p'a_1^L D_1 \geq p'a_1^L \left[ a_2^L \langle N_d \rangle / p - a_0^U \langle N_s \rangle / p' - (a_2^L a_0^U - a_2^L a_0^U) \langle D_0 \rangle \right] / a_1^L a_2^L - a_1^L a_2^L \]  

(55)

and \( \langle N_d \rangle \) and \( \langle N_s \rangle \) are defined by equations (50) and (53). The range of \( \langle D_0 \rangle \) is given by fact 2 where the range of \( \langle D_0 \rangle \) is given by equation (51). To have the lower bound value of \( n'_{1s} \) in equation (54), we only need to put the smallest value of \( \langle N_d \rangle \) and the largest possible values of \( \langle N_s \rangle, \langle D_0 \rangle \) into equation (55). However, we do not use the largest possible value of \( \langle D_0 \rangle \), because we only need the worst-case result of the final key rate rather than the worst-case result in each step.

According to these, we can lower bound the fraction of single-photon counts of the raw bits caused by signal pulses through the equation

\[ \Delta_1' \geq \frac{\tilde{n}'_{1s}}{N_s}. \]  

(56)

where \( \tilde{n}'_{1s} \) is defined in equation (54) and the ranges of related variables in equation (54) can be calculated by equations (50), (51), (53), (55) and fact 2, if the conditions of equations (26) and (36) hold.

For coherent states, if the intensity is bounded by \([\mu^L, \mu^U]\) for the decoy pulses and \([\mu'^L, \mu'^U]\) for the signal pulses, then

\[ a_k^X = (\mu^X)^k e^{-\mu^X} / k!, \quad a_k^X = (\mu'^X)^k e^{-\mu'^X} / k! \]  

with \( X = L, U \) and \( k = 1, 2 \) and

\[ a_0^L = e^{-\mu^U}, \quad a_0^U = e^{-\mu^L}; \quad a_0'^L = e^{-\mu'^U}, \quad a_0'^U = e^{-\mu'^L}. \]  

(57)

Note that our result is not limited to a coherent state source. To calculate the unconditionally secure final key rate, one has to combine our result (equation (56)) with the existing theory of finite-size QKD [4, 6, 7]. Here we make a loose treatment to show the effects of our equation (56) on the key rate by adding statistical fluctuation to \( t \) and \( t_1 \) in equation (4). Detailed numerical results using the experimental data of QKD over 102.7 km calculated by our formula are listed in table 1. We treat the experimental data in the following way for the key rate of signal pulses by equation (4): (i) \( \Delta_1' \) can be calculated by equation (56) as stated earlier. (ii) Half of the experimental data of signal pulses should be discarded due to the measurement basis mismatch.
Table 1. Secure key rate (final bits per pulse in units of $10^{-6}$) versus intensity error upper bound using the experimental data in the case of 102.7 km [22]. The first row lists different values of upper bounds of intensity errors, $\delta_M$, i.e. when we want an intensity $x$, we can actually create a pulse of any intensity in the range $[x(1 - \delta_M), x(1 + \delta_M)]$. Other rows list the final key rates, which are the numbers of final bits per signal pulse after error test, i.e. $n_{f\tilde{N}_s}$ where $\tilde{N}_s$ is the number of raw bits of signal pulses after error test and $n_f$ is the number of final bits distilled from these $\tilde{N}_s$ raw bits. $R$ is the asymptotic key rate; $R_1$, $R_2$ and $R_3$ are the non-asymptotic key rates with the intensity of each pulse in $Y_0$ being bounded by 0, 0.5 and 1%, respectively. The intensity fluctuations of any decoy pulses and signal pulses are bounded by $\delta_M$. In the table, we have given the results of key rate, while $\delta_M$ ranges from 0 to 3%.

| $\delta_M$ | 3%  | 2.5% | 2%  | 1.5% | 1%  | 0.5% | 0%  |
|------------|-----|------|-----|------|-----|------|-----|
| $R$ (in $10^{-6}$) | 11.03 | 12.09 | 13.15 | 14.19 | 15.23 | 16.26 | 17.28 |
| $R_1$ (in $10^{-6}$) | 1.536 | 2.567 | 3.591 | 4.607 | 5.616 | 6.618 | 7.614 |
| $R_2$ (in $10^{-6}$) | 1.506 | 2.537 | 3.561 | 4.577 | 5.587 | 6.589 | 7.585 |
| $R_3$ (in $10^{-6}$) | 1.475 | 2.507 | 3.531 | 4.548 | 5.557 | 6.560 | 7.556 |

in the BB84 protocol. (iii) Among the remaining half, a quarter are consumed for the bit-flip test and another quarter are consumed for the phase-flip test. (iv) We use $t_0 = t_0(\mu') = 3.580\%$ as the observed value of both bit-flip rate and phase-flip rate. The final key is distilled from the remaining bits of signal pulses. The number of the remaining bits is not less than $\tilde{n}_{1s}/4$. We use $t = t_0(\mu')$ for the bit-flip rate, and

$$t_1 = t_0' + 10\sqrt{4t_0'/\tilde{n}_{1s}}.$$  \hspace{1cm} (59)

$\tilde{n}_{1s}$ is given by equation (54), and

$$t_0' = \frac{t_0 - \mu'\Delta_1D_0}{2\tilde{N}_0}.$$  \hspace{1cm} (60)

We then put all possible values of $D_0$ into equation (4) according to fact 2 and equation (51) for the worst-case result of key rate over $D_0$.

The detailed experimental parameters can be found in [22]. For completeness, we list the main parameters here in table 2.

4. Some remarks on source errors

By existing technology, one can indeed use whatever stabilizer to reduce the source errors considerably. Even then, our theoretical results are still necessary. Firstly, no technology can guarantee a perfectly stable source. It is also questionable whether any existing device has been proven to be able to reduce the source errors to a low level, which is exponentially close to 0. If unconditional security is our goal in practice, we must show quantitatively the effects of any polynomial imperfections. For example, even if we can control the intensity fluctuation to
Table 2. Main parameters and observed results in the experiment of [22]. $M$: total pulses sent out by Alice during the experimental time. $t_0(\mu), t_0(\mu')$: QBER of decoy pulses and signal pulses. $S', S, S_0$: counting rates of signal pulses, decoy pulses and $Y_0$ pulses. From the results listed in table 1, we find that the effects of source errors on the key rate are not significant (provided that the source error is not too large). For example, in the asymptotic case (results in the first row), if the largest intensity fluctuation is controlled to be less than 0.5%, the key rate is decreased from 17.28 Hz (the data in the last column of the first row) to 16.26 Hz only (data in the second column from the right of the first row). However, the statistical fluctuation decreases the key rate significantly, given the existing experiment [22]. If we strictly considered the finite-size effect [4, 6, 7], the key rate would be further decreased. To reduce the effects, one can increase the number of pulses in the setup.

| $M$ | $t_0(\mu')$ | $t_0(\mu)$ | $S'$ | $S$ | $S_0$ | $p'$ | $p$ | $p_0$ |
|-----|-------------|-------------|------|------|------|------|------|------|
| 5.222 $\times 10^9$ | 3.580% | 9.098% | 1.262 $\times 10^{-4}$ | 4.611 $\times 10^{-5}$ | 6.711 $\times 10^{-6}$ | 0.5 | 0.4 | 0.1 |

be less than 0.5%, we had better still consider the effects of intensity fluctuation quantitatively rather than simply trust that the effects are negligible by intuition. Otherwise, one may ask why the cut-off point is 0.5% rather than 0.0001 or 25%? The security is then standardless. If we disregard the effect of source errors, possibly we shall encounter the following ridiculous story: setup A produces a key rate of 1 k s$^{-1}$ with source errors of less than 0.5% and setup B produces a key rate of 20 k s$^{-1}$ with source errors of 25% over the same distance. Do we have to believe that setup B is better? With our theoretical results, such a type of issue is immediately resolved because we can calculate the net final key rate after considering the effects of source errors. Secondly, with our theoretical results, we do not have to blindly take too much costs in improving the source quality. For example, with our results we now know with strict proof that source intensity fluctuation less than 0.0001% is not so necessary, since it only improves the key rate negligibly, if we can already control errors less than 0.5%. Finally, there are cases when Eve can indeed know the intensity errors [28]. As explicitly shown in [10, 28], in such cases Eve can then violate equation (3) by producing a time-dependent channel transmittance. The situation of the Plug-and-Play is even more serious: Eve can actually prepare the error of each pulse and then she can violate equation (3) for sure.

5. Concluding remark and discussions

In summary, we have shown how to calculate the lower bound of the fraction of single-photon counts in the decoy-state QKD with both source errors and statistical fluctuations. By our method, all imperfections have been taken into consideration in the largest possible errors of a few parameters of the source states in photon number space. Therefore we only need to know the bound values of a few parameters of sources instead of assuming exact values of any physical quantity. For example, we do not have to assume zero internal fluctuation of Alice’s attenuation as assumed by earlier works [27, 29].
Obviously, our result here directly applies to the so-called Plug-and-Play protocol first proposed by Gisin et al as pointed out in [30]. Combined with the decoy state method with two-way quantum communication [31], the protocol [2, 30] can be made secure if Alice’s attenuation can be accurately set [29, 32]. By our results here, Gisin’s Plug-and-Play protocol [2] can be secure even if Alice cannot set her attenuation accurately. In the Plug-and-Play protocol, Eve actually knows the error of each individual pulse; hence the error-free decoy-state theory based on equation (3) fails but our theory works here. There, Alice receives strong pulses from Bob and she needs to guarantee the exact intensity of the pulse sending to Bob. It is not difficult to check the intensity, but difficult to precisely correct the intensity of each individual pulse. Our theory here can help to make it easier [28]: Alice monitors each pulse. She may either choose to do crude corrections to the pulses or not do any corrections. She simply discards those pulses whose intensity errors are too large (e.g. beyond 2%), and then uses our theory to distill the final key.

It should be interesting to combine our result with existing theories on final key distillation in a finite size QKD [4, 6, 7] for the unconditional final key rate in the finite-size decoy-state QKD with an unstable source.

Acknowledgment

This work was supported in part by the National Basic Research Program of China grant nos 2007CB907900 and 2007CB807901, NSFC grant nos 60725416, 60525201 and 60708023, and China Hi-Tech program grant no. 2006AA01Z420.

Appendix

For simplicity, we consider those pulses containing 10 photons when flying into Alice’s lab and, after Alice’s attenuation, containing 1 photon when flying away from Alice’s lab to Bob. Alice decides to randomly use her transmittance $\lambda = \lambda^D = 0.01$ to produce a signal pulse and $\lambda = \lambda^S = 0.05$ to produce a signal pulse. However, due to whatever uncontrolled cause, there are internal fluctuations of the $\lambda$ value at different times. Consider the following specific case: to some blocks of pulses (we call these blocks strong blocks), to all decoy pulses and signal pulses, the real transmittance is a bit larger than $\lambda$, the value that Alice wants, while in some other blocks (we call weak blocks) the real transmittance is a bit smaller than $\lambda$. Suppose the numbers of pulses in the strong blocks and in the weak blocks are equal. In the strong blocks, Alice’s real transmittance for a decoy pulse or a signal pulse is $\lambda^{D+} = 1.01\lambda^D$ or $\lambda^{S+} = 1.01\lambda^D$, whereas in the weak blocks, Alice’s real transmittance for a decoy pulse or a signal pulse is $\lambda^{D-} = 0.99\lambda^D$ or $\lambda^{S-} = 0.99\lambda^S$. Suppose every block contains millions of pulses; therefore Eve can know whether a block is a strong block or a weak block by observing the averaged intensity of pulses in the block. That is to say, Eve can treat different blocks differently. Eve produces a channel transmittance of $\eta^+$ to each pulse in the strong blocks and another transmittance $\eta^-$ to each pulse in weak pulses. Note that here Eve does not know which pulses are decoy pulses and which pulses are signal pulses. She treats all pulses in one block in a fixed way. Now we can directly calculate $Y_{10,1}^D$ and $Y_{10,1}^S$:

$$Y_{10,1}^D = \frac{\lambda^{D+}(1 - \lambda^{D+})^9 \eta^+ + \lambda^{D-}(1 - \lambda^{D-})^9 \eta^-}{\lambda^{D+}(1 - \lambda^{D+})^9 + \lambda^{D-}(1 - \lambda^{D-})^9} = \frac{1.01(1 - 1.01\lambda^D)^9 \eta^+ + 0.99(1 - 0.99\lambda^D)^9 \eta^-}{1.01(1 - 1.01\lambda^D)^9 + 0.99(1 - 0.99\lambda^D)^9},$$

(A.1)
\[ Y_{10,1}^{S} = \frac{\lambda S^+ (1 - \lambda S^+) \eta^+ + \lambda S^- (1 - \lambda S^-) \eta^-}{\lambda S^+ (1 - \lambda S^+) + \lambda S^- (1 - \lambda S^-)} = \frac{1.01 (1 - 0.1 \lambda S^+ \eta^+ + 0.99 (1 - 0.99 \lambda S^-) \eta^-}{1.01 (1 - 0.1 \lambda S^+ \eta^+ + 0.99 (1 - 0.99 \lambda S^-) \eta^-} \]  

(A.2)

It is easy to see that in general \( Y_{10,1}^{D} = Y_{10,1}^{S} \) if \( \eta^+ = \eta^- \). For example, given that \( \eta^+ = 5 \eta^- \), numerical calculation shows that

\[ \frac{Y_{10,1}^{D}}{Y_{10,1}^{S}} > 1.0025. \]  

(A.3)

This counterexample shows clearly that in principle the assumption \( Y_{m,n}^{D} = Y_{m,n}^{S} \) is incorrect if Alice’s transmittance is not exactly controlled. Obviously, such a case is equivalent to saying that the pulse intensity from Alice is inexact; this is just the case we have studied in [28]. As was clearly shown there and also in [10], Eve can produce different transmittances for the single-photon state from the decoy source and the signal source. If Alice can control the attenuation exactly, i.e. \( \lambda^D, \lambda^S \), there exists a more efficient way of managing the issue in the protocol of one-way quantum communication [27]. Our counterexample here is not in conflict with the derivations in [29] because there Alice’s attenuation is assumed to be stable.

References

[1] Bennett C H and Brassard G 1984 Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (New York: IEEE) pp 175–9
[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Rev. Mod. Phys. 74 145
[3] Dusek M, Lütkenhaus N and Hendrych M 2006 Progress in Optics VVVX ed E Wolf (Amsterdam: Elsevier)
[4] Inamori H, Lütkenhaus N and Mayers D 2007 Eur. Phys. J. D 41 599 (arXiv:quant-ph/0107017)
[5] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 Eur. Phys. J. D 41 599 (arXiv:quant-ph/0107017)
[6] Scarani V and Renner R 2008 Phys. Rev. Lett. 100 302008
[7] Scarani V and Renner R 2008 3rd Workshop on Theory of Quantum Computation, Communication and Cryptography (TQC 2008), (University of Tokyo, Tokyo 30 Jan–1 Feb 2008) See also arXiv:0806.0120
[8] Raymond Cai Y Q and Scarani V 2009 New J. Phys. 11 045024 (arXiv:0811.2628)
[9] Huttner B, Imoto N, Gisin N and Mor T 1995 Phys. Rev. A 51 1863
[10] Yuen H P 1996 Quantum Semiclass. Opt. 8 939
[11] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 Phys. Rev. Lett. 85 1330
[12] Lütkenhaus N 2000 Phys. Rev. A 61 052304
[13] Lütkenhaus N and Jahn M 2002 New J. Phys. 4 44
[14] Wang X-B, Hiroshima T, Tomita A and Hayashi M 2007 Phys. Rep. 448 1
[15] Hwang W-Y 2003 Phys. Rev. Lett. 91 057901
[16] Wang X-B 2005 Phys. Rev. Lett. 94 230503
[17] Wang X-B 2005 Phys. Rev. A 72 012322
[18] Lo H-K, Ma X and Chen K 2005 Phys. Rev. Lett. 94 230504
[19] Wang X-B 2005 Phys. Rev. A 72 012322
[20] Harrington J W et al 2005 arXiv:quant-ph/0503002
[21] Mauerer W and Silberhorn C 2007 Phys. Rev. A 75 050305
[22] Adachi Y, Yamamoto T, Koashi M and Imoto N 2008 Phys. Rev. Lett. 99 180503
[23] Hirikiri T and Kobayashi T 2006 Phys. Rev. A 73 032331
[24] Wang Q, Wang X-B and Guo G-C 2007 Phys. Rev. A 75 012312
[25] Hayashi M 2007 New J. Phys. 9 248

New Journal of Physics 11 (2009) 075006 (http://www.njp.org/)
[18] Ursin R et al 2006 arXiv:quant-ph/0607182
[19] Scarani V, Acin A, Ribordy G and Gisin N 2004 Phys. Rev. Lett. 92 057901
    Branciard C, Gisin N, Kraus B and Scarani V 2005 Phys. Rev. A 72 032301
[20] Koashi M 2004 Phys. Rev. Lett. 93 120501
    Tamaki K, Lükenhaus N, Loashi M and Batuwantudawe J 2006 arXiv:quant-ph/0608082
[21] Rosenberg D et al 2007 Phys. Rev. Lett. 98 010503
[22] Peng C-Z et al 2007 Phys. Rev. Lett. 98 010505
[23] Schmitt-Manderbach T et al 2007 Phys. Rev. Lett. 98 010504
[24] Yuan Z-L, Sharpe A W and Shields A J 2007 Appl. Phys. Lett. 90 011118
    Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shields A J 2008 Opt. Express 16 18790
[25] Tanaka A et al 2008 Opt. Express 16 11354
[26] Wang X-B 2007 Phys. Rev. A 75 012301
[27] Wang X-B, Peng C-Z and Pan J-W 2007 Appl. Phys. Lett. 90 031110
[28] Wang X-B, Peng C-Z, Zhang J, Yang L and Pan J-W 2008 Phys. Rev. A 77 042311
[29] Zhao Y et al 2008 Phys. Rev. A 77 052327
[30] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 Phys. Rev. A 73 022320
[31] Zhao Y, Qi B, Ma X, Lo H-K and Qian L 2006 Phys. Rev. Lett. 96 070502
    Zhao Y, Qi B, Ma X, Lo H-K and Qian L 2006 Proc. IEEE Int. Symp. on Information Theory (Seattle)
    (New York: IEEE) pp 2094–8
[32] Peng X et al 2008 Opt. Lett. 33 2077