Twin-Field Quantum Key Distribution with large random intensity fluctuation

Feng-Yu Lu,1,2 Zhen-Qiang Yin,1,2 Chao-Han Cui,1,2 Guan-Jie Fan-Yuan,1,2 Shuang Wang,1,2 De-Yong He,1,2 Wei Chen,1,2 Guang-Can Guo,1,2 and Zheng-Fu Han1,2

1 Key Laboratory of Quantum Information, CAS Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China
2 State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China

Twin-Field Quantum Key Distribution (TFQKD) Protocol and its variants, such as Phase-Matching QKD (PM-QKD), sending or not QKD (SNS-QKD) and No Phase Post-Selection TFQKD (NPP-TFQKD) can overcome the rate-distance limited without the help of quantum repeaters and they also close all loopholes on measurement detector. However, those protocols still rely on security hypothesis of source side. Using decoy state method, we can estimate the upper and lower bound of yield of n-photon state and calculate the secure key rate of the protocol even if we don’t have ideal single photon source. This method require accurate controlling of each decoy intensity. However, there usually exist random intensity fluctuations on source side, which bring secure loophole on source side. In this article, We present a theoretical model to close this loophole in NPP-TFQKD. Firstly, we present an analytical formula of 4-intensity decoy state method of NPP-TFQKD since the linear program method will be invalid when the intensities of decoy states are uncertain. Then based on the analytical formula, we give a countermeasure to intensity fluctuation in NPP-TFQKD. The simulation results show that, by using our method, intensity fluctuations have very limited influence on the performance of TF-QKD, which implies the robustness of this protocol in practice.

* yinzq@ustc.edu.cn
I. INTRODUCTION

Quantum Key Distribution (QKD) \[1,2\] is one of the most successful applications in quantum information science. It allows two remote users, called Alice and Bob, to share random secret keys even if there is an eavesdropper, Eve. It’s information-theoretic security has been proved for many decades\[3–5\]. These proofs rely on the hypothesis of the absolute security on detector side and source side. However, there are large gaps between ideal and practical devices. On source side, ideal single photon source is not yet practically useful and modulators are not ideal since noise, time jitter and problems of modulation signals etc. On detector side, there have been many proven attacks aim at imperfection of single photon detector\[6,7\].

To remove all detector side loopholes, Measurement-Device-Independent Quantum Key Distribution (MDI-QKD)\[8–11\] which immune to all fatal attacks on detector side was proposed\[6,7\]. To deal with the imperfection of source side, people presented decoy method\[12–17\] to estimate the yield and error rate of single photon state. With the help of decoy method, the achievable distance of QKD is significantly improved even if we use weak coherent state (WCS) source rather than ideal single photon source.

Except for these efforts on closing gaps between theoretical and practical devices, QKD implementations with longer achievable distance\[18,19\] and higher secret key rate (SKR)\[20–22\] were realized. However, all these implementations must obey some limits on SKR versus channel transmittance\[23,24\]. Moreover, SKR of any "repeater-less" QKD system cannot overcome the linear bound (also called PLOB bound)\[23\]. Surprisingly, a recently proposed protocol called Twin-Field Quantum Key Distribution (TF-QKD)\[25\] and its variants\[26,27\], e.g., Phase-Matching QKD (PM-QKD)\[27\], Sending-or-Not QKD (SNS-QKD)\[28\] and TF-QKD without phase post-selection (we will call it NPP-TFQKD in the following, which is the abbreviation of no phase post-Selection TF-QKD\[29–31\]) can overcome this bound, which means the performance of QKD may be significantly improved without the need of quantum repeaters.

These TF-QKD protocols have been proved to be immune to all potential side-channel attacks to measurement device, just like the original measurement-device-independent protocol\[8–11\]. But some loopholes are remained on source side. The problem of intensity fluctuation\[32–34\] is one of them. When using decoy state method, we have to accurately control intensity of each decoy state since we need these intensity values to estimate the yield and error rate of n-photon states. The problem is that, the intensity of WCS is very difficult to be controlled exactly. In this paper, we present a method to re-calculate SKR of NPP-TFQKD\[29\] when there is large random intensity fluctuation in source side. We firstly present an analytical formula of 4-intensity decoy method, since the traditional linear program (we will call it numerical formulor in the following) is invalid when the intensities are uncertain. Inspired by the model proposed by Ref.[33], we will propose a improved method to deal with intensity fluctuation. The new method can calculate upper and lower bound of any of n-photon state probability and the bound is tighter. The model without any assumption about the intensity distribution only need to know average intensity and fluctuation range of each decoy states. According to our simulation results, the SKR and achievable distance are only slightly lost and the protocol still can break the linear bound even if the intensity fluctuation is upper bounded by ±100%.

The rest of this paper is organized as followeing. Since the traditional numerical methods are invalid when intensities are uncertain, in Sec.II, we we will present an analytical formula of 4-intensity decoy method NPP-TFQKD and give its proof. In Sec.III, we will introduce our intensity fluctuation model and analize the SKR-distance relation in different fluctuation ranges.

II. ANALYTICAL FORMULA OF 4-INTENSITY DECOY METHOD NPP-TFQKD

Our work is based on 4-intensity decoy method NPP-TFQKD proposed in Ref.[29]. We will firstly review the flow of this protocol as following.

Step 1. In each trial, Alice and Bob randomly choose code mode or decoy mode quantum state to send to untrusted Charlie to do measurement.

Step 2. In code mode, Alice(Bob) prepares a phase coding weak coherent pulse whose initial global phase is locked.

In decoy mode, Alice(Bob) randomly chooses an intensity νa(νb) from a pre-decided set and prepares a
phase randomized WCS. Alice(Bob) actually prepares a mixed state since the randomized phase in decoy mode will never be publicly announced. The density matrix can be denoted as Eq.(1)

$$\rho_{\nu} = \sum_{n=0}^{\infty} e^{-\nu} \frac{\nu^n}{n!} |n\rangle\langle n|$$ (1)

**Step 3.** For each trail. The untrusted Charlie must publicly announce the detector 'L' or 'R' that click or failure. The click will be called success event in the following.

**Step 4.** Alice and Bob repeat above steps sufficient times, then they publicly announce which trails are code mode and which are decoy mode. For the trials they both choose code mode and Charlie announce success event, the raw key bits are generated. According to Charlie’s announcement, Bob may need to flip his raw key bit.

**Step 5.** Alice and Bob accumulate data to estimate the gain and quantum bit error rate(QBER) of trials they both send code mode and they use formula of decoy state method to estimate the upper bound of information leakage. Then they use those estimated values to do error correction and privacy amplification to generate their secure key.

The SKR per trial is given in Eq(2), where $Q_{\mu}$ and $E_{\mu}$ are, respectively, gain and QBER of the code mode. $H(p) = -p \log_2 p - (1 - p) \log_2 (1 - p)$ is Shannon entropy. $I_{AE}$ can describe the information leakage which can be estimate by yield of n-photon state $Y_{nm}$. The $Y_{nm}$ denotes the yield when Alice send n-photon state and Bob send m-photon state. The details of $I_{AE}$ can be found in Ref.[20].

$$R = Q_{\mu}[1 - f H(E_{\mu}) - I_{AE}^n]$$ (2)

Firstly, we will discribe our motivation to build the analytical formula. To estimate the upper bound of $I_{AE}$, we have to firstly estimate the upper bound of $q_{00}$, $q_{10}$, $q_{01}$, $q_{20}$, $q_{02}$, $q_{11}$ and lower bound of $q_{nm} = q_{00} + q_{10} + q_{01} + q_{20} + q_{02} + q_{11}$ by decoy state method[24] where $q_{nm} = p_{nm}^{E_{\mu}} Y_{nm}$. $p_{nm}^{E_{\mu}} = e^{-x(y)n}$ is the possibility of n-photon state in x-intensity phase randomized WCS. When using linear program, we have to solve a equation set consist of equations showed in Eq.(3), where $Q_{xy}$ is the gain when Alice and Bob choose intensity x and y respectively. $x(y) \in \mu, \nu, \omega, o$. we should estimate the upper and lower bound of $Y_{nm}$ form equation set Eq.(3). Because $p_{nm}^{E_{\mu}}$ depends on the intensity x, it’s obviously that the linear program will be not valid any more if the intensity, in other word, the coefficients $p_{nm}^{E_{\mu}}$ in Eq.(3) are uncertain.

$$Q_{xy} = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} p_{nm}^{E_{\mu}} Y_{nm}; \quad x, y \in \{\mu, \nu, \omega, o\}$$ (3)

It’s intuitive that, even though there is large intensity fluctuation, when using analytical formula, we can still get secure bound of key rate if we correctly replace coefficients $p_{nm}^{E_{\mu}}$ in the formula by $\overline{p_{nm}^{E_{\mu}}}$ or $\underline{p_{nm}^{E_{\mu}}}$ Thus we present a analytical formula before building the fluctuation model. We will use overline and underline to express, respectively, upper and lower bound of a variable.

Before prove our analytical formula, we should define some symbols and give an important equation showed in Eq.(4) [16, 17] which will be frequently used in the following. The intensity in code mode is $\mu$ and intensities in decoy mode are $\mu, \nu, \omega$ and $o$(the largest intensity in decoy mode is the same as code mode). $\mu > \nu > \omega > o$ and $o = 0$ is the vacuum state. Define $a_n = p_n^\mu$, $b_n = p_n^\nu$, $c_n = p_n^\omega$.

$$\frac{p_m^\mu}{p_m^{\nu}} \geq \frac{p_n^\mu}{p_n^{\nu}} \quad (\mu \geq \nu ; \quad m \geq n)$$ (4)

**Step 1** $q_{00}$:

$Y_{00} = Q_{00}$ since $p_0^\nu = 1$, then $q_{00} = a_0^2 Y_{00}$.

**Step 2** $\overline{y}_{01}$ and $\underline{y}_{10}$:
We take $q_{01}$ as an example. Firstly, we define $K_1 = Q_{o\mu} - a_0 Q_{oo} = \sum_{n=1}^{\infty} a_n Y_{0n}$, $K_2 = Q_{o\nu} - b_0 Q_{oo} = \sum_{n=1}^{\infty} b_n Y_{0n}$, $K_4 = Q_{o\nu} - c_0 Q_{oo} = \sum_{n=1}^{\infty} c_n Y_{0n}$ and $\tau = \sum_{k=3}^{\infty} b_k Y_{0k}$.

Combining with Eq. (11), we can obtain a set of inequalities as showed in Eq. (5).

\[
\begin{cases}
  K_1 b_3/a_3 > a_1 b_3 Y_{01}/a_3 + a_2 b_3 Y_{02}/a_3 + \tau \\
  K_2 = b_1 Y_{01} + b_2 Y_{02} + \tau \\
  K_3 b_3/c_3 < c_1 b_3 Y_{01}/c_3 + c_2 b_3 Y_{02}/c_3 + \tau
\end{cases}
\]  

(5)

Solve Eq. (5), we obtain the upper bound of $Y_{01}$.

\[
Y_{01} = \frac{K_2 (c_2 a_3 - c_3 a_2) + K_1 (b_2 c_3 - b_3 c_2) + K_3 (a_2 b_3 - a_3 b_2)}{2(b_1 c_3 - c_1 a_3) + b_1 (c_2 a_3 - c_3 a_2) + b_3 (a_2 c_1 - a_1 c_2)}
\]  

(6)

$g_{01} = a_0 a_1 Y_{01}$. 

Step 3. $q_{02}$ and $q_{20}$:  
We take $q_{02}$ as an example. Using Eq. (8) We obtain a set of inequalities as showed in Eq. (7). Where $H_1 = Q_{o\mu} - a_0 Q_{oo}$ and $L_3 = Q_{o\nu} - c_0 Q_{oo} - (1 - \sum_{k=0}^{2} c_k)$.

\[
\begin{cases}
  H_1 > Y_{01} a_1 + Y_{02} a_2 \\
  L_3 < Y_{01} c_1 + Y_{02} c_2
\end{cases}
\]  

(7)

Solve Eq. (7), we obtain the upper bound of $Y_{02}$

\[
Y_{02} < \frac{H_1 c_1 - L_3 a_1}{a_2 c_1 - a_1 c_2} = \overline{Y}_{02}
\]  

(8)

$g_{02} = a_0 a_2 Y_{02}$

Step 4. $q_{11}$:  
It’s easily to calculate $q_{11}$ by using $Q_{\mu,\mu}$, $Q_{\mu,o}$, $Q_{o,\mu}$ and $Q_{o,o}$.

\[
q_{11} < \sum_{m=1, n=1}^{\infty} Y_{mn} = Q_{\mu,\mu} - a_0 Q_{\mu,o} - a_0 Q_{o,\mu} + (a_0)^2 Q_{oo} = \overline{Y}_{11}
\]  

(9)

Step 5. $q_{sum}$:  
Here, $q_{sum} = \sum_{n=0}^{2} \sum_{m=0}^{2-m} q_{nm}$. We define $q_{sum} = t_1 + t_2$, where $t_1 = q_{00} + q_{01} + q_{10} + q_{20}$ and $t_2 = q_{11}$.

We can easily estimate $t_1$ by Eq. (10)

\[
t_1 = a_0 [Q_{o\mu} + Q_{o\nu} - 2(1 - a_0 - a_1 - a_2)] - (a_0)^2 Q_{oo}
\]  

(10)

Then we calculate the lower bound of $Y_{11}$. similar to the step.1, we can obtain an equation set, i.e. Eq. (11), where $K_1 = Q_{\mu,\mu} - a_0 (Q_{o\mu} + Q_{\mu,\nu}) + (a_0)^2 Q_{o,o}$, $K_2 = Q_{\nu,\nu} - a_0 (Q_{o\nu} + Q_{\nu,\nu}) + (a_0)^2 Q_{oo}$ and $\tau' = \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} b_m b_n Y_{m,n} - (b_1)^2 Y_{1,1}$.

\[
\begin{cases}
  \frac{K_1 b_1 b_2}{a_1 a_2} < \frac{a_1 b_1 b_2 Y_{1,1}}{a_2} + \tau' \\
  K_2 = (b_1)^2 Y_{1,1} + \tau'
\end{cases}
\]  

(11)
Solve the Eq.(11), we obtain the $Y_{11}$.

\[
Y_{11} = \frac{K_1 b_1 b_2 - K_2 a_1 a_2}{a_1^2 b_1 b_2 - b_2^2 a_1 a_2} 
\]

Finally, $q_{num} = \mu_1 + \mu_2 = \mu_1 + a_1^2 Y_{11}$.

Using these estimated $Y_{nm}$, we can calculate the upper bound of information leakage $I_{AE}$ according to method proposed in Ref.[29].

The comparation of our analytical formula and numerical method in Ref.[29] is showed in Fig.1. The parameters are showed in Tab.I.

FIG. 1. SKR versus distance between Alice and Bob, the blue solid line is the numerical method of 4-intensity decoy method proposed in Ref.[29], the red dash line is our analytical method and the yellow dot-dash line is linear bound.

III. NPP-TFQKD WITH LARGE RANDOM INTENSITY FLUCTUATION

It’s obviously that decoy method relys on the knowledge of the density matrix showed in Eq.(1) of each decoy state. The coefficients of each fock state $|n\rangle\langle n|$ in Eq.(1) are unknown quantities when the intensity of each decoy states are uncertain. In this situation, the decoy method will lose its power. An intuitive idea is using analytical formula and correctly replacing all coefficients(in our formula are $a_n$, $b_n$ and $c_n$) by their upper or lower bound. However, this replacement leads to intolerable loss of SKR and reachable distance. In this section, we will present an improved intensity fluctuation model based on Ref.[33]. The model doesn’t require any assumption about intensity distribution. It only needs to know the average intensity and fluctuation range which can be measured by proven techniques[33]. Our model is suitable for any of n-number state and can bound the possibility coefficients $p^n_x$ tighter.

| $p_{dc}$ | $\eta_d$ | $f$ | fiber loss | $\nu$ | $\omega$ |
|----------|----------|-----|------------|-----|--------|
| $8 \times 10^{-8}$ | 14.5% | 1.15 | 0.2 dB/km | 0.004 | 0.001 |
By using our method, the NPP-TFQKD with large random fluctuation on source side can still overcome the rate-distance linear bound. We will introduce our model in the following.

![Graph of SKR versus distance between Alice and Bob with different fluctuation ranges.](image)

**FIG. 2.** SKR versus distance between Alice and Bob with different fluctuation ranges, the blue solid line is the our analytical method with no intensity fluctuation, the red, yellow and purple dash line are, respectively, the fluctuation range of 20%, 50% and 100%. The green dot-dash line is linear bound.

Firstly, we should define some symbols. Let’s take the first decoy state(intensity is $\mu$) as an example.

Since the random fluctuation, when we want sent $\mu$-intensity weak coherent pulse, we prepare $\mu_i = \hat{\mu}(1 + \delta_i)$, $\hat{\mu}$ is the expectation intensity. $\overline{\delta}$ and $\underline{\delta}$ are, respectively, maximum and lower minimum fluctuation. i.e. $\mu^\pm = \hat{\mu}(1 + \delta^\pm)$

the density matrix of the source with fluctuation can be describe by Eq.(13)

$$\rho'_{\mu} = \sum_{i=1}^{\infty} \sum_{n=0}^{\infty} e^{-\mu_i} \frac{\mu^n}{n!} |n\rangle \langle n| / N$$

The probability of emit $n$-photon state is re-write as $a_n = \frac{\mu^n e^{-\hat{\mu}}}{n! N} \sum_{i=1}^{N \to \infty} e^{-\delta_i \hat{\mu}} (1 + \delta_i)^n$

Using taylor expansion, we get Eq.(14)

$$a_n = \frac{\mu^n e^{-\hat{\mu}}}{n! N} \sum_{i=1}^{N \to \infty} (1 - \delta_i \hat{\mu} + (\delta_i \hat{\mu})^2 / 2! - ...) (1 + C_n^1 \delta_i + C_n^2 (\delta_i)^2 + ...)

= \frac{\mu^n e^{-\hat{\mu}}}{n! N} \left[1 + \sum_{i=1}^{N \to \infty} (n - \hat{\mu}) \delta_i + o(\delta_i)\right]$$

Noting a important fact that $\sum_{i=1}^{N \to \infty} \delta_i = 0$, we find the first order item of $\delta$ is not exist in Eq.(14). i.e, the Eq.(14) can be re-written as Eq.(15)

$$a_n = \frac{\mu^n e^{-\hat{\mu}}}{n! N} \sum_{i=1}^{N \to \infty} e^{-\delta_i \hat{\mu}} (1 + \delta_i)^n - \sum_{i=1}^{N \to \infty} (n - \hat{\mu}) \delta_i$$

Defining function $f_\mu^n(\delta) = e^{-\delta \hat{\mu}} (1 + \delta)^n - (n - \hat{\mu}) \delta$, $\delta \in [\overline{\delta}, \underline{\delta}]$. $f_\mu^n(\delta^\pm)$ are, respectively, maximum and minimum value in range of $[\overline{\delta}, \underline{\delta}]$. $\delta^\pm$ are maximum and minimum value points. $\delta^\pm$ can be easily found by
optimization algorithms. Since \( a_n = \frac{1}{n!} \sum_{i=1}^{N} f_n^i (\delta_i) \), we get a new tighter bound of \( a_n \) as showed in Eq.(16).

\[
\overline{a}_n = \frac{1}{n!} \sum_{i=1}^{N} f_n^i (\delta^+) \quad a_n = \frac{1}{n!} f_n^h (\delta^-)
\] (16)

Replacing all possibility coefficients by their tighter bound in analytical formula, we get the new bound of \( q_{nm} \) as following.

**Step.1 upper bound of \( q_{00} \):**

\( q_{00} = \overline{a}_{00} \)

**Step.2 New upper bound of \( q_{10} \) and \( q_{01} \):** We take \( \overline{q}_{10} \) as example, the \( \overline{q}_{01} \) is similar.

\[
\overline{q}_{10} = \frac{\overline{a}_{10}}{\overline{a}_{00}} \overline{a}_{00} \quad \overline{a}_{00} = \frac{1}{n!} f_n^h (\delta^-)
\]

The \( K_1 = Q_{\mu o} - \overline{a}_{00} Q_{oo} \), \( K_2 = Q_{\nu o} - b_0 Q_{oo} \) and \( K_3 = Q_{\omega o} - \overline{a}_0 Q_{oo} \).

**Step.3 New upper bound of \( q_{20} \) and \( q_{02} \):**

We take \( \overline{q}_{20} \) as example.

\[
\overline{q}_{20} = \frac{\overline{a}_{20}}{\overline{a}_{00}} \overline{a}_{00} \quad \overline{a}_{00} = \frac{1}{n!} f_n^h (\delta^-)
\]

Here, \( \overline{H}_1 = Q_{\mu o} - \overline{a}_0 Q_{oo} \), \( \overline{L}_1 = Q_{\omega o} - \overline{a}_0 Q_{oo} \), \( \overline{L}_1 = (\sum_{n=3}^{\infty} a_n) - \overline{a}_0 Q_{oo} \).

**Step.4 New upper bound of \( q_{11} \):**

\[
\overline{q}_{11} = Q_{\mu \mu} - \overline{a}_0 (Q_{oo} + Q_{\mu o}) + \overline{a}_0^2 Q_{oo}
\]

**Step.5 New lower of \( q_{sum} \):**

\[
q_{sum} = l_1 + l_2
\]

\[
l_1 = \omega_0 (Q_{oo} + Q_{\mu o} - 2 \sum_{n=3}^{\infty} a_n) - \overline{a}_0 Q_{oo}
\]

\[
l_2 = \frac{\overline{a}_0^2 (Q_{oo} + Q_{\mu o}) - \overline{a}_0 Q_{oo}}{\overline{a}_0 \overline{a}_{00} - \overline{a}_0^2 \overline{a}_{00}}
\]

We simulate the SKR-distance relation with different fluctuation range by simulation. The result is showed in Fig.(2) and Fig(3). The parameters choosing is showed in Tab.(I). By using the model, NPP-TFQKD can still break the linear bound even if the fluctuation range is as large as 100%.

![SKR versus intensity fluctuation](image)

**FIG. 3.** SKR versus intensity fluctuation. The x-axis is fluctuation range, y-axis is SKR. Different colors denote different distance between Alice and Bob as show in legend.

7
IV. DISCUSSION

In this article, we firstly present the analytical formula of 4-intensity decoy state method of NPP-TFQKD. Then, we present an improved fluctuation model based on the model proposed in Ref. [33]. Our model can calculate the possibility bound of any of n-photons and it can estimate a tighter bound.

In summary, combining our analytical formula and fluctuation model, we can re-calculate the SKR when there are random intensity fluctuations in source side. Simulations show that intensity fluctuations have very limited influence on the performance of TF-QKD, which implies the robustness of this protocol in practice.

V. FUNDING INFORMATION

This work has been supported by the National Key Research And Development Program of China (Grant Nos. 2016YFA0302600 and 2016YFA0301702), the National Natural Science Foundation of China (Grant Nos. 61775207, 61627820, 61622506, 61575183, and 61675189), the â€œStrategic Priority Research Program (B)â€ of the Chinese Academy of Sciences (Grant No. XDB01030100), Foundation of Science and Technology on Communication Security Laboratory (6142103040105).

APPENDIX A: ESTIMATION OF INFORMATION LEAKAGE

Before introduce the $I_{AE}$, we should define some physical quantities. $|\gamma_{n,m}\rangle$ is the state of Eve’s ancilla in case of Alice and Bob sending Fock states $|n\rangle$ and $|m\rangle$ respectively. $|\psi_{ee}\rangle$, $|\psi_{oe}\rangle$, $|\psi_{eo}\rangle$ and $|\psi_{oo}\rangle$ are intermediate states labeled by the photon-number’s parity of Alice and Bob’s output which showed in Eq.(A.17).

\begin{align}
|\psi_{ee}\rangle &= \sum_{n,m} \sqrt{\frac{p_{2n}^2 p_{2m}^2}{Q_{2n,2m}}} |\gamma_{2n,2m}\rangle \\
|\psi_{oe}\rangle &= \sum_{n,m} \sqrt{\frac{\mu_{2n+1}^2 p_{2m}^2}{Q_{2n+1,2m}}} |\gamma_{2n+1,2m}\rangle \\
|\psi_{eo}\rangle &= \sum_{n,m} \sqrt{\frac{p_{2n+1}^2 \mu_{2m+1}^2}{Q_{2n+1,2m+1}}} |\gamma_{2n+1,2m+1}\rangle \\
|\psi_{oo}\rangle &= \sum_{n,m} \sqrt{\frac{\mu_{2n+1}^2 \mu_{2m+1}^2}{Q_{2n+1,2m+1}}} |\gamma_{2n+1,2m+1}\rangle \\
\end{align}

(A.17)

The theoretical bound of $I_{AE}$ is showed in Eq.(A.18)

$$I_{AE} \leq h(\frac{||\psi_{ee}||^2}{Q_{\mu}}, \frac{||\psi_{oe}||^2}{Q_{\mu}}) + h(\frac{||\psi_{oo}||^2}{Q_{\mu}}, \frac{||\psi_{eo}||^2}{Q_{\mu}})$$

However, as described in Ref. [29], if we apply finite decoy states, we can only obtain good bound of several $Y_{nm}$ with small $n$ and $m$. We have to use another formula to bound the $I_{AE}$. Since the proof can be found in Ref. [29], we only introduce the final result here.

The upper bound of $I_{AE}$ is

$$T_{AE} = \max h(\frac{x_{ee}}{Q_{\mu}}, \frac{x_{oe}}{Q_{\mu}}) + h(\frac{x_{oo}}{Q_{\mu}}, \frac{x_{eo}}{Q_{\mu}});$$

(A.19)

The variables $x_{ee}$, $x_{oe}$, $x_{eo}$ and $x_{oo}$ in Eq. (A.19) are restricted by Eq. (A.20), where ‘e’ denotes ‘even’ and ‘o’ denotes ‘odd’.
\[ x_{ee} \leq \max_{k \geq 2} \left| \sqrt{q_{00}} + \sqrt{q_{02}} + \sqrt{q_{20}} + \sum_{n=2}^{+\infty} \sum_{i=0}^{n} \sqrt{p_{2i}^\mu p_{2(n-i)}^\mu} \right| \]
\[ \frac{(k + 4)(k - 1)}{2} (Q_\mu - \sum_{n=k+1}^{+\infty} \sum_{i=0}^{n} p_{2i+1}^\mu p_{2(n-i)}^\mu - q_{\text{num}}) \right|^2; \]
\[ x_{oe} \leq \max_{k \geq 1} \left| \sqrt{q_{1,0}} + \sum_{n=k+1}^{+\infty} \sum_{i=0}^{n} \sqrt{p_{2i+1}^\mu p_{2(n-i)+1}^\mu} \right| \]
\[ \frac{(k + 3)k}{2} (Q_\mu - \sum_{n=k+1}^{+\infty} \sum_{i=0}^{n} p_{2i+1}^\mu p_{2(n-i)+1}^\mu - q_{\text{num}}) \right|^2; \]
\[ x_{co} \leq \max_{k \geq 1} \left| \sqrt{q_{1,1}} + \sum_{n=k+1}^{+\infty} \sum_{i=0}^{n} \sqrt{p_{2i+1}^\mu p_{2(n-i)+1}^\mu} \right| \]
\[ \frac{(k + 3)k}{2} (Q_\mu - \sum_{n=k+1}^{+\infty} \sum_{i=0}^{n} p_{2i+1}^\mu p_{2(n-i)+1}^\mu - q_{\text{num}}) \right|^2; \]
\[ x_{oo} \leq \max_{k \geq 1} \left| \sqrt{q_{1,1}} + \sum_{n=k+1}^{+\infty} \sum_{i=0}^{n} \sqrt{p_{2i+1}^\mu p_{2(n-i)+1}^\mu} \right| \]
\[ \frac{(k + 3)k}{2} (Q_\mu - \sum_{n=k+1}^{+\infty} \sum_{i=0}^{n} p_{2i+1}^\mu p_{2(n-i)+1}^\mu - q_{\text{num}}) \right|^2; \]
\[ x_{00} + x_{10} + x_{11} + x_{01} = Q_\mu. \]

[1] C. H. Bennett and G. Brassard, Theor. Comput. Sci. 560, 7 (2014).
[2] A. K. Ekert, Physical review letters 67, 661 (1991).
[3] D. Mayers, Journal of the ACM (JACM) 48, 351 (2001).
[4] H.-K. Lo and H. F. Chau, science 283, 2050 (1999).
[5] P. W. Shor and J. Preskill, Physical review letters 85, 441 (2000).
[6] V. Makarov, New Journal of Physics 11, 065003 (2009).
[7] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Physical review A 78, 042333 (2008).
[8] H.-K. Lo, M. Curty, and B. Qi, Physical review letters 108, 130503 (2012).
[9] C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, Physical review letters 115, 160502 (2015).
[10] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, et al., Physical review letters 111, 130502 (2013).
[11] X. Ma and M. Razavi, Physical review A 86, 062319 (2012).
[12] W.-Y. Hwang, Physical Review Letters 91, 057901 (2003).
[13] H.-K. Lo, X. Ma, and K. Chen, Physical review letters 94, 230504 (2005).
[14] X.-B. Wang, Physical review A 72, 012322 (2005).
[15] X.-B. Wang, Physical review letters 94, 230503 (2005).
[16] X.-B. Wang, Physical review A 87, 012320 (2013).
[17] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Physical Review A 91, 032318 (2015).
[18] A. Boaron, G. Bosco, D. Rusca, C. Vulliez, C. Autebert, M. Calez, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, et al., Physical review letters 121, 190502 (2018).
[19] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, et al., Physical review letters 117, 190501 (2016).
[20] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, Optics letters 37, 1008
[21] K. J. Gordon, V. Fernandez, G. S. Buller, I. Rech, S. D. Cova, and P. D. Townsend, Optics Express 13, 3015 (2005).

[22] S. Wang, W. Chen, Z.-Q. Yin, D.-Y. He, C. Hui, P.-L. Hao, G.-J. Fan-Yuan, C. Wang, L.-J. Zhang, J. Kuang, et al., Optics letters 43, 2030 (2018).

[23] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. 8, 15043 (2017).

[24] M. Takeoka, S. Guha, and M. M. Wilde, Nat. Commun 5, 5235 (2014).

[25] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, Nature 557, 400 (2018).

[26] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, arXiv preprint arXiv:1805.05511 (2018).

[27] X. Ma, P. Zeng, and H. Zhou, arXiv preprint arXiv:1805.05538 (2018).

[28] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Physical Review A 98, 062323 (2018).

[29] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, arXiv preprint arXiv:1807.02334 (2018).

[30] M. Curty, K. Azuma, and H.-K. Lo, arXiv preprint arXiv:1807.07667 (2018).

[31] J. Lin and N. Lütkenhaus, Physical Review A 98, 042332 (2018).

[32] X.-B. Wang, L. Yang, C.-Z. Peng, and J.-W. Pan, New Journal of Physics 11, 075006 (2009).

[33] X.-B. Wang, Physical Review A 75, 052301 (2007).

[34] X.-Y. Zhou, C.-M. Zhang, and Q. Wang, JOSA B 34, 1518 (2017).