Measurement-device-independent quantum cryptographic conferencing with an untrusted source*

Rui-Ke Chen(陈瑞柯)[1,2], Wan-Su Bao(鲍皖苏)[1,2,†], Yang Wang(汪洋)[1,2], Hai-Ze Bao(包海泽)[1,2], Chun Zhou(周淳)[1,2], Mu-Sheng Jiang(江木生)[1,2], and Hong-Wei Li(李宏伟)[1,2]

[1] *Zhengzhou Information Science and Technology Institute, Zhengzhou* 450001, *China*

[2] *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*

(Received 11 July 2016; revised manuscript received 20 September 2016; published online 29 November 2016)

Measurement-device-independent quantum cryptographic conferencing (MDI-QCC) protocol puts MDI quantum key distribution (MDI-QKD) forwards to multi-party applications, and suggests a significant framework for practical multi-party quantum communication. In order to mitigate the experimental complexity of MDI-QCC and remove the key assumption (the sources are trusted) in MDI-QCC, we extend the framework of MDI-QKD with an untrusted source to MDI-QCC and give the rigorous security analysis of MDI-QCC with an untrusted source. What is more, in the security analysis we clearly provide a rigorous analytical method for parameters' estimation, which with simple modifications can be applied to not only MDI-QKD with an untrusted source but also arbitrary multi-party communication protocol with an untrusted source. The simulation results show that at reasonable distances the asymptotic key rates for the two cases (with trusted and untrusted sources) almost overlap, which indicates the feasibility of our protocol.

Keywords: quantum cryptographic conferencing, measurement-device-independent, quantum key distribution, untrusted source

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/26/1/010302

1. Introduction

Quantum communication has been developed in the past thirty years. One highlighted communication protocol is quantum key distribution (QKD).[1] QKD is to allow two authorized parties, Alice and Bob, to share a secret key in the presence of an eavesdropper. QKD offers unconditional security guaranteed by the laws of quantum mechanics.[2–4] However, real-life imperfections of the QKD devices lead to the difference between theoretical and practical security of QKD, which compromises the security of QKD systems. In order to close the gap, device-independent QKD (DIQKD)[5–7] and semi-device-independent QKD (SDI-QKD)[8,9] have been proposed. Unfortunately, the demonstration of these two protocols is still an extremely difficult challenge.

As we know, among the real-life imperfections, the defect in the detectors is a serious threat to the security. By exploiting the vulnerabilities of single-photon detectors, several specific attacks[10–17] have been successfully launched against practical QKD systems. Fortunately, measurement-device-independent QKD (MDI-QKD)[18,19] has been proposed, which can remove all the possible loopholes in detection. Thereafter, MDI-QKD has drawn great interest in both theory[20–31] and experiment.[32–40]

All the protocols mentioned above are two-party protocols distributing secret keys between two authorized parties. Multi-party quantum communication protocols[41,42] have been proposed. But all of them face the same constraints, i.e., lacking the high intensity source and reliable remote distribution of the entangled states. Until recently, two multi-party quantum communication protocols[43,44] combining the MDI-QKD[18,19] technologies manifest the possibility for the practical applications of MDI multi-party quantum communication. These two protocols are not only immune to all detection-side attacks, but also require neither the preparation of high-fidelity entangled states (GHZ states or W states) in advance nor their remote distribution. Afterwards, a finite-key analysis on MDI quantum cryptographic conferencing (MDI-QCC)[43] has been reported in Ref. [45].

However, just like in MDI-QKD system, there are still some major challenges making the practical applications of MDI-QCC[43,44] an experimental challenge. Firstly, we assume there is no security loophole in the users' frequency-locked lasers. Secondly, a complex time-synchronization system and feedback controls are truly essential in fiber communication. Thirdly, in MDI-QCC protocol, it also needs to ensure the indistinguishability of the particles from Alice, Bob, and Charlie. However, since the photons are prepared independently, it is difficult to meet this condition.

Recently, Xu[29] has proposed an MDI-QKD protocol with a single untrusted source and provided a complete security analysis. This protocol can overcome the analogous challenges mentioned above in MDI-QKD. It should be noted that

*Project supported by the National Basic Research Program of China (Grant No. 2013CB338002) and the National Natural Science Foundation of China (Grant Nos. 11304397 and 61505261).

†Corresponding author. E-mail: 2010thzz@sina.com

in the decoy-analysis of MDI-QKD with an untrusted source, Xu uses the numerical method to study the precise parameters' estimation and just presents a relatively simple analytical method.

In this paper, we extend the framework of MDI-QKD with an untrusted source to MDI-QCC and give a complete security analysis. Due to the bi-directional structure, the birefringence effects and polarization-dependent losses can be automatically compensated. With a single source, we can easily ensure the indistinguishability of the particles from different users. What is more, inspired by the security analysis for plug & play QKD,[46,47] we give a rigorous analytical method for parameters' estimation based on the actual photon number distribution of users' output pulses.

2. MDI-QCC with an untrusted source

To extend the protocol of MDI-QKD with an untrusted source[29] to MDI-QCC, we clearly define the protocol of MDI-QCC with an untrusted source illustrated in Fig. 1. Here, we clarify the required assumptions for our protocol. First, we require that Alice's, Bob's, and Charlie's laboratories are perfectly isolated, and their devices are independent. Second, Alice's, Bob's, and Charlie's monitoring devices are trusted. The monitoring unit used in our protocol is realized by a standard optical filter and a classical intensity detector. So most of the attacks against single-photon detectors are ineffective. The security of the intensity detector has been studied in Ref. [48]. Then, the detailed description of our protocol is presented below.

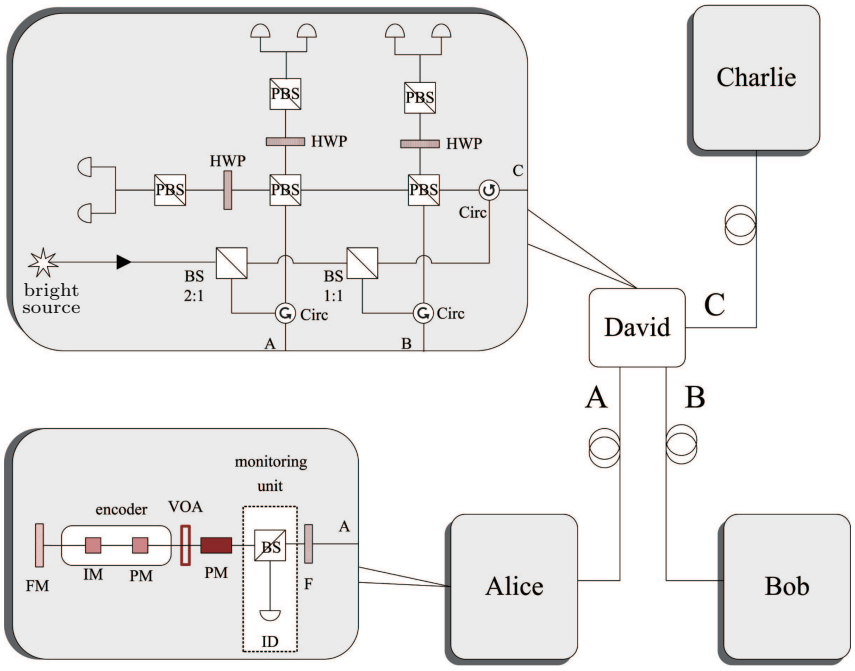

Fig. 1. (color online) Schematic layout of the MDI-QCC with an untrusted source setup. An untrusted relay, David, generates bright laser pulses. They are split into three parts by two beam splitters (BS). Before entering Alice's, Bob's, and Charlie's lab, the pulses will travel through the channel, which is fully controlled by Eve. In the lab, to ensure the single mode assumption for each signal, the pulses pass through an optical filter (F) first. After that, a monitoring unit, which consists of a BS and an intensity detector (ID), is needed to monitor the photon number distribution of the input pulse. Then, the input pulses pass through a phase modulator (PM) for phase randomization, a variable optical attenuator (VOA) and an encoder that consists of an intensity modulator (IM) and a PM. Finally, the pulses are reflected by a Faraday mirror (FM) and travel back to David who is supposed to perform a GHZ-state measurement.[43] The measurement can identify two of the eight GHZ states.

(i) State preparation and distribution David, located in the middle node, generates bright pulses whose photon numbers are centered at $M_{\rm d}$. The bright pulses go through two beam splitters one after another and are split into three parts. Then, David sends them to Alice, Bob, and Charlie via two quantum channels. In this paper, we assume a fiber-based channel model.

(ii) Monitoring and encoding The pulses sent by David suffer the whole channel loss and then enter Alice's, Bob's, and Charlie's lab. In the lab, to remove side-channels and ensure that only pulses of the desired mode can pass through, we place an optical filter working in spectral, spatial, and temporal domains. Accordingly, the single mode assumption for each pulse sustains. Then, the pulses go through a monitoring unit which consists of a $q/(1-q)$ beam splitter and an intensity monitor. The monitoring unit is used to estimate the photon number of input pulses.[29] After the monitoring unit, the pulses go through a phase modulator used to apply the phase randomization on each pulse. The randomization is used to disentangle the input pulse into a classical mixture of Fock states, which is also the foundation of our security analysis. Then, the input pulses are encoded by an encoder which consists of a phase modulator (PM) and an intensity modulator (IM). After that, the pulses are reflected by a Faraday mirror

(FM).

(iii) Measurement The reflected pulses are attenuated to the single-photon level by a variable optical attenuator. We denote the internal transmittance of Alice's, Bob's, and Charlie's labs as $\lambda_s^{\gamma_s}(s=\mathrm{a},\mathrm{b},\mathrm{c})$, where the superscript $\gamma_s \in \{u,v,0\}$ are the intensity settings chosen by Alice, Bob, and Charlie, and the subscripts $s=\mathrm{a},\mathrm{b},\mathrm{c}$ refer to Alice, Bob, and Charlie respectively. Then, the attenuated pulses retransmit through the same optical fiber to David. David is supposed to perform a GHZ-state measurement which can identify two of the eight GHZ states, that is, $\left|\Phi_0^+\right\rangle = 1/\sqrt{2}\,(|HHH\rangle + |VVV\rangle)$ and $\left|\Phi_0^-\right\rangle = 1/\sqrt{2}\,(|HHH\rangle - |VVV\rangle)$.

(iv) Sifting David reveals which GHZ state he has obtained. Meanwhile, Alice, Bob, and Charlie broadcast the intensity settings and post-select the events where they use the same basis via an authenticated channel.

(v) Parameter estimation The data of Z basis are used to generate the cryptographic conferencing keys, while the data of X basis are totally used to estimate errors. Alice, Bob, and Charlie estimate the gain and quantum bit error rate of single-photon pulses of untagged pulses with the decoy state method.

(vi) Post processing Firstly, Alice, Bob, and Charlie apply the error correction to ensure that they share a string of identical keys. Secondly, to make the leakage of information on keys as little as possible, they apply the privacy amplification to extract the secret key.

Here, in order to post-select GHZ states among Alice, Bob, and Charlie, we need to ensure the mode matching of their pulses. Since we use plug-and-play architecture in our protocol, the polarization drift can be automatically compensated, and the spectral modes of these pulses are naturally identical. So the only measure we need to take is to actively control the arrival timing of the pulses.

3. Properties of untagged pulses

As the framework presented in Section 2, the source is placed in the middle node. So we can consider the source is controlled by Eve. To enhance the security of our protocol, we place an optical filter and phase modulator in the users' lab to ensure the single mode assumption and phase randomization on each input pulse, respectively. In addition, the monitoring unit in users' lab is used to test the photon numbers of the input pulses. In order to estimate the bounds of output pulses, we focus on the input pulses whose photon numbers are concentrated in a relatively narrow range.

Following Ref. [29], we divide the input pulses into two categories according to the photon numbers: untagged input pulses with photon number $m_s \in [(1-\delta_s)M_s,(1+\delta_s)M_s]$, and tagged input pulses with photon number $m_s < (1-\delta_s)M_s$ or $m_s > (1+\delta_s)M_s$, where the subscript $s=\mathrm{a},\mathrm{b},\mathrm{c}$ denotes which users (Alice, Bob, or Charlie) the pulses belong to. $\delta_s(s=\mathrm{a},\mathrm{b},\mathrm{c})$ is a small positive real number, chosen in advance by Alice, Bob, and Charlie. $M_s(s=\mathrm{a},\mathrm{b},\mathrm{c})$ is a large positive integer denoted as the average of the photon numbers of the input pulses. For a specific user (Alice, Bob, or Charlie), these parameters can be denoted as $\{m_\mathrm{a},\delta_\mathrm{a},M_\mathrm{a}\}$, $\{m_\mathrm{b},\delta_\mathrm{b},M_\mathrm{b}\}$, or $\{m_\mathrm{c},\delta_\mathrm{c},M_\mathrm{c}\}$.

The conditional probability that n_a $(n_\mathrm{b},n_\mathrm{c})$ photons are emitted by Alice (Bob, Charlie) given that m_a $(m_\mathrm{b},m_\mathrm{c})$ photons entering Alice's (Bob's, Charlie's) device obeys a binomial distribution as

$$P_{n_s}^{\gamma_s}(m_s) = C_{m_s}^{n_s}(\lambda_s^{\gamma_s}q)^{n_s}(1-\lambda_s^{\gamma_s}q)^{m_s-n_s}, \quad s=\mathrm{a},\mathrm{b},\mathrm{c}, \tag{1}$$

where $\lambda_s^{\gamma_s}(s=\mathrm{a},\mathrm{b},\mathrm{c})$ are the internal transmittance of Alice's, Bob's, and Charlie's labs when their intensity settings are $\gamma_s \in \{u,v,0\}(s=\mathrm{a},\mathrm{b},\mathrm{c})$, respectively, and q is the splitting ratio of the beam splitter in Alice's, Bob's, and Charlie's monitoring units.

For untagged pulses, we can show that the upper bound and lower bound of $P_{n_s}^{\gamma_s}(m_s)(s=\mathrm{a},\mathrm{b},\mathrm{c})$ are

$$\begin{aligned}
\overline{P_{n_s}^{\gamma_s}(m_s)} &= \begin{cases} (1-\lambda_s^{\gamma_s}q)^{(1-\delta_s)M_s}, & \text{if } n_s=0,\\ C_{(1+\delta_s)M_s}^{n_s}(\lambda_s^{\gamma_s}q)^{n_s}(1-\lambda_s^{\gamma_s}q)^{(1+\delta_s)M_s-n_s}, & \text{if } 1\le n_s\le(1+\delta_s)M_s,\\ 0, & \text{if } n_s>(1+\delta_s)M_s, \end{cases}\\
\underline{P_{n_s}^{\gamma_s}(m_s)} &= \begin{cases} (1-\lambda_s^{\gamma_s}q)^{(1+\delta_s)M_s}, & \text{if } n_\alpha=0,\\ C_{(1-\delta_s)M_s}^{n_s}(\lambda_s^{\gamma_s}q)^{n_s}(1-\lambda_s^{\gamma_s}q)^{(1-\delta_s)M_s-n_s}, & \text{if } 1\le n_s\le(1-\delta_s)M_s,\\ 0, & \text{if } n_s>(1-\delta_s)M_s. \end{cases}
\end{aligned} \tag{2}$$

In practice, quantum non-demolition (QND) measurements on photon number of the input pulses are not feasible with current technology. Thus Alice, Bob, and Charlie do not know the exact photon number of each input pulse. They can only measure the overall gain Q_e and the overall quantum bit error rate (QBER) E_e, and cannot get the gain Q and the QBER EQ of the untagged pulses directly. However, as in the description of the protocol presented in Sec-

tion 2, Alice, Bob, and Charlie can use a monitoring unit to sample the input pulses to acquire information about the photon number distribution. From Ref. [29], with this information, Alice, Bob, and Charlie know that at least $(1-\Delta_{\rm a}-\varepsilon_{\rm a})k$, $(1-\Delta_{\rm b}-\varepsilon_{\rm b})k$, and $(1-\Delta_{\rm c}-\varepsilon_{\rm c})k$ pulses are untagged with high confidence, where k denotes the number of pulses sent by David and $\Delta_{\rm a}$ $(\Delta_{\rm b},\Delta_{\rm c})$ denotes the probability that a certain sampling pulse of Alice (Bob, Charlie) belongs to untagged pulses in the asymptotic case. In the asymptotic case, $\varepsilon_{\rm a},\varepsilon_{\rm b},\varepsilon_{\rm c}\sim 0$. The calculating methods of $\Delta_{\rm a}$ $(\Delta_{\rm b},\Delta_{\rm c})$ are totally presented in Ref. [29], which have been elided here for brevity.

Then Alice, Bob, and Charlie can estimate the upper bounds and the lower bounds of the gain Q and the QBER EQ of the untagged pulses. The upper bound and lower bound of Q are given by

$$\overline{Q}=\frac{Q_e}{(1-\Delta_{\rm a}-\varepsilon_{\rm a})(1-\Delta_{\rm b}-\varepsilon_{\rm b})(1-\Delta_{\rm c}-\varepsilon_{\rm c})},\quad \underline{Q}=\max\left(0,\frac{Q_e-1+(1-\Delta_{\rm a}-\varepsilon_{\rm a})(1-\Delta_{\rm b}-\varepsilon_{\rm b})(1-\Delta_{\rm c}-\varepsilon_{\rm c})}{(1-\Delta_{\rm a}-\varepsilon_{\rm a})(1-\Delta_{\rm b}-\varepsilon_{\rm b})(1-\Delta_{\rm c}-\varepsilon_{\rm c})}\right). \tag{3}$$

The upper bound and lower bound of EQ are given by

$$\overline{EQ}=\frac{Q_eE_e}{(1-\Delta_{\rm a}-\varepsilon_{\rm a})(1-\Delta_{\rm b}-\varepsilon_{\rm b})(1-\Delta_{\rm c}-\varepsilon_{\rm c})},\quad \underline{EQ}=\max\left(0,\frac{Q_eE_e-1+(1-\Delta_{\rm a}-\varepsilon_{\rm a})(1-\Delta_{\rm b}-\varepsilon_{\rm b})(1-\Delta_{\rm c}-\varepsilon_{\rm c})}{(1-\Delta_{\rm a}-\varepsilon_{\rm a})(1-\Delta_{\rm b}-\varepsilon_{\rm b})(1-\Delta_{\rm c}-\varepsilon_{\rm c})}\right). \tag{4}$$

4. Security analysis

If the source is trusted, Eve only knows the output photon number n_s $(s={\rm a,b,c})$ of each pulse. This draws out the basic assumption of previous decoy state analysis of MDI-QCC, that is,

$$Y^S_{n_{\rm a,b,c}}=Y^D_{n_{\rm a,b,c}},e^S_{n_{\rm a,b,c}}=e^D_{n_{\rm a,b,c}},$$

where the subscript $n_{\rm a,b,c}$ denotes that the photon numbers of the output pulses of Alice, Bob, and Charlie are $n_{\rm a},n_{\rm b},n_{\rm c}$, respectively.

However, if the source is untrusted, the assumption above no longer holds. Because both the source and channel are controlled by Eve, Eve not only knows the output photon number n_s $(s={\rm a,b,c})$, but also knows the input photon number m_s $(s={\rm a,b,c})$. In this case, $Y^S_{n_{\rm a,b,c}}\neq Y^D_{n_{\rm a,b,c}}$ and $e^S_{n_{\rm a,b,c}}\neq e^D_{n_{\rm a,b,c}}$. Considering m_s and n_s jointly, we can find that

$$Y^S_{m_{\rm a,b,c}n_{\rm a,b,c}}=Y^D_{m_{\rm a,b,c}n_{\rm a,b,c}},e^S_{m_{\rm a,b,c}n_{\rm a,b,c}}=e^D_{m_{\rm a,b,c}n_{\rm a,b,c}},$$

where the subscript $m_{\rm a,b,c}n_{\rm a,b,c}$ denotes that the photon numbers of the input pulses and the output pulses of Alice, Bob, and Charlie are $m_{\rm a},m_{\rm b},m_{\rm c}$ and $n_{\rm a},n_{\rm b},n_{\rm c}$, respectively.

In this case, the rigorous decoy-state analysis for MDI-QCC with untrusted source becomes much more difficult and complicated. Fortunately, since we focus on the gain and the QBER of the untagged pulses whose photon numbers are concentrated within a narrow range, the unconditional security of our protocol can still be achieved quantitatively and rigorously. By performing the measurements for different intensity settings, we can obtain

$$\begin{aligned}Q^{\chi}_{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}&=\sum_{m_{\rm a},m_{\rm b},m_{\rm c}}\sum_{n_{\rm a},n_{\rm b},n_{\rm c}}P(m_{\rm a}m_{\rm b}m_{\rm c},n_{\rm a}n_{\rm b}n_{\rm c})\\&\quad\times Y_{m_{\rm a,b,c}n_{\rm a,b,c}},\end{aligned} \tag{5}$$

$$\begin{aligned}E^{\chi}_{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}Q^{\chi}_{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}&=\sum_{m_{\rm a},m_{\rm b},m_{\rm c}}\sum_{n_{\rm a},n_{\rm b},n_{\rm c}}P(m_{\rm a}m_{\rm b}m_{\rm c},n_{\rm a}n_{\rm b}n_{\rm c})\\&\quad\times Y_{m_{\rm a,b,c}n_{\rm a,b,c}}e_{m_{\rm a,b,c}n_{\rm a,b,c}},\end{aligned} \tag{6}$$

where $P(m_{\rm a}m_{\rm b}m_{\rm c},n_{\rm a}n_{\rm b}n_{\rm c})$ denotes the joint probability that the input (output) photon numbers of Alice, Bob, and Charlie are $m_{\rm a},m_{\rm b},m_{\rm c}$ $(n_{\rm a},n_{\rm b},n_{\rm c})$, respectively; $\chi\in\{X,Z\}$ denotes that Alice, Bob, and Charlie choose the same basis (X or Z). According to the multiplication theorems on probability, we have $P(m_{\rm a}m_{\rm b}m_{\rm c},n_{\rm a}n_{\rm b}n_{\rm c})=P_{\rm in}(m_{\rm a}m_{\rm b}m_{\rm c})P^{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}_{n_{\rm a}n_{\rm b}n_{\rm c}}(m_{\rm a}m_{\rm b}m_{\rm c})$, where $P_{\rm in}(m_{\rm a}m_{\rm b}m_{\rm c})$ denotes the joint probability that Alice's, Bob's, and Charlie's input pulses contain m_s $(s={\rm a,b,c})$ photons, and $P^{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}_{n_{\rm a}n_{\rm b}n_{\rm c}}(m_{\rm a}m_{\rm b}m_{\rm c})$ denotes the conditional probability that $n_{\rm a},n_{\rm b},n_{\rm c}$ photons are emitted by Alice, Bob, and Charlie given that $m_{\rm a},m_{\rm b},m_{\rm c}$ photons enter Alice's, Bob's, and Charlie's devices. So, Eqs. (5) and (6) can be written as

$$\begin{aligned}Q^{\chi}_{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}&=\sum_{m_{\rm a},m_{\rm b},m_{\rm c}}\sum_{n_{\rm a},n_{\rm b},n_{\rm c}}P_{\rm in}(m_{\rm a}m_{\rm b}m_{\rm c})\\&\quad\times P^{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}_{n_{\rm a}n_{\rm b}n_{\rm c}}(m_{\rm a}m_{\rm b}m_{\rm c})Y_{m_{\rm a,b,c}n_{\rm a,b,c}},\end{aligned} \tag{7}$$

$$\begin{aligned}E^{\chi}_{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}Q^{\chi}_{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}&=\sum_{m_{\rm a},m_{\rm b},m_{\rm c}}\sum_{n_{\rm a},n_{\rm b},n_{\rm c}}P_{\rm in}(m_{\rm a}m_{\rm b}m_{\rm c})\\&\quad\times P^{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}_{n_{\rm a}n_{\rm b}n_{\rm c}}(m_{\rm a}m_{\rm b}m_{\rm c})Y_{m_{\rm a,b,c}n_{\rm a,b,c}}e_{m_{\rm a,b,c}n_{\rm a,b,c}}.\end{aligned} \tag{8}$$

Because the events that $n_{\rm a}$ $(n_{\rm b},n_{\rm c})$ photons are emitted by Alice (Bob, Charlie) given that $m_{\rm a}$ $(m_{\rm b},m_{\rm c})$ photons have entered Alice's (Bob's, Charlie's) device are independent, we have

$$P^{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}_{n_{\rm a}n_{\rm b}n_{\rm c}}(m_{\rm a}m_{\rm b}m_{\rm c})=P^{\gamma_{\rm a}}_{n_{\rm a}}(m_{\rm a})P^{\gamma_{\rm b}}_{n_{\rm b}}(m_{\rm b})P^{\gamma_{\rm c}}_{n_{\rm c}}(m_{\rm c}).$$

Thus, equations (7) and (8) can be written as

$$\begin{aligned}Q^{\chi}_{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}&=\sum_{m_{\rm a},m_{\rm b},m_{\rm c}}\sum_{n_{\rm a},n_{\rm b},n_{\rm c}}P_{\rm in}(m_{\rm a}m_{\rm b}m_{\rm c})\\&\quad\times P^{\gamma_{\rm a}}_{n_{\rm a}}(m_{\rm a})P^{\gamma_{\rm b}}_{n_{\rm b}}(m_{\rm b})P^{\gamma_{\rm c}}_{n_{\rm c}}(m_{\rm c})Y_{m_{\rm a,b,c}n_{\rm a,b,c}},\end{aligned} \tag{9}$$

$$E^{\chi}_{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}Q^{\chi}_{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}=\sum_{m_{\rm a},m_{\rm b},m_{\rm c}}\sum_{n_{\rm a},n_{\rm b},n_{\rm c}}P_{\rm in}(m_{\rm a}m_{\rm b}m_{\rm c})P^{\gamma_{\rm a}}_{n_{\rm a}}(m_{\rm a})$$

$$\times P_{n_{\rm b}}^{\gamma_{\rm b}}(m_{\rm b}) P_{n_{\rm c}}^{\gamma_{\rm c}}(m_{\rm c}) Y_{m_{\rm a,b,c} n_{\rm a,b,c}} e_{m_{\rm a,b,c} n_{\rm a,b,c}}. \quad (10)$$

4.1. The gain of single-photon pulses of untagged pulses

To estimate the gain of single-photon pulses of untagged pulses, we have to solve Eq. (9) under the constraints of the binomial probability distributions given by Eq. (2). From the proof in Appendix A, the lower bound of untagged pulses Q_{111}^{Z} is given by

$$\underline{Q_{111}^{Z}} = \underline{P_{111}^{uuu}} \left(\frac{\underline{Q_{vvv}^{Z}}\,\underline{P_{222}^{uuu}} - \overline{Q_{uuu}^{Z}}\,\overline{P_{222}^{vvv}}}{\overline{P_{111}^{vvv}}\,\underline{P_{222}^{uuu}} - \underline{P_{111}^{uuu}}\,\overline{P_{222}^{vvv}}} + \frac{(\underline{P_{000}^{uuu}}\,\overline{P_{222}^{vvv}} - \overline{P_{000}^{vvv}}\,\underline{P_{222}^{uuu}})\,\overline{Q_{000}^{Z}}}{\overline{P_{111}^{vvv}}\,\underline{P_{222}^{uuu}} - \underline{P_{111}^{uuu}}\,\overline{P_{222}^{vvv}}} \right),$$

where Q_{uuu}^{Z} (Q_{vvv}^{Z}, Q_{000}^{Z}) are the gain of single-photon pulses of untagged pulses when Alice, Bob, and Charlie choose the signal state (the decoy state, the vacuum state) simultaneously, and their bounds can be estimated from Eq. (3). Then,

$$\begin{aligned} \underline{P_{n_{\rm a} n_{\rm b} n_{\rm c}}^{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}} &= \underline{P_{n_{\rm a}}^{\gamma_{\rm a}}} \cdot \underline{P_{n_{\rm b}}^{\gamma_{\rm b}}} \cdot \underline{P_{n_{\rm c}}^{\gamma_{\rm c}}}, \\ \overline{P_{n_{\rm a} n_{\rm b} n_{\rm c}}^{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}} &= \overline{P_{n_{\rm a}}^{\gamma_{\rm a}}} \cdot \overline{P_{n_{\rm b}}^{\gamma_{\rm b}}} \cdot \overline{P_{n_{\rm c}}^{\gamma_{\rm c}}}, \end{aligned} \quad (11)$$

where $\overline{P_{n_s}^{\gamma_s}}(s = {\rm a,b,c})$ and $\underline{P_{n_s}^{\gamma_s}}(s = {\rm a,b,c})$ are defined by Eq. (2). We have $\underline{P_{000}^{uuu}} = \underline{P_0^{u_{\rm a}}} \cdot \underline{P_0^{u_{\rm b}}} \cdot \underline{P_0^{u_{\rm c}}}$, $\underline{P_{111}^{uuu}} = \underline{P_1^{u_{\rm a}}} \cdot \underline{P_1^{u_{\rm b}}} \cdot \underline{P_1^{u_{\rm c}}}$, $\underline{P_{222}^{uuu}} = \underline{P_2^{u_{\rm a}}} \cdot \underline{P_2^{u_{\rm b}}} \cdot \underline{P_2^{u_{\rm c}}}$, $\overline{P_{000}^{uuu}} = \overline{P_0^{u_{\rm a}}} \cdot \overline{P_0^{u_{\rm b}}} \cdot \overline{P_0^{u_{\rm c}}}$, $\overline{P_{111}^{uuu}} = \overline{P_1^{u_{\rm a}}} \cdot \overline{P_1^{u_{\rm b}}} \cdot \overline{P_1^{u_{\rm c}}}$, and $\overline{P_{222}^{uuu}} = \overline{P_2^{u_{\rm a}}} \cdot \overline{P_2^{u_{\rm b}}} \cdot \overline{P_2^{u_{\rm c}}}$, where $\underline{P_0^{u_{\rm a}}}$, $\underline{P_1^{u_{\rm a}}}$, $\underline{P_2^{u_{\rm a}}}$, $\overline{P_0^{u_{\rm a}}}$, $\overline{P_1^{u_{\rm a}}}$, and $\overline{P_2^{u_{\rm a}}}$ are defined by Eq. (2).

4.2. The error rate of single-photon pulse of untagged pulses

To estimate the error rate of single-photon pulses of untagged pulses, we have to solve Eq. (10) under the constraints of the binomial probability distributions given by Eq. (2). From the proof in Appendix B, the upper bound of e_{111}^{X} in untagged pulses is given by

$$\begin{aligned} e_{111}^{X} \le\ & \frac{1}{\underline{P_{111}^{vvv}} \cdot \underline{V_{111}}} (\overline{E_{vvv}^{X} Q_{vvv}^{X}} - \underline{P_0^{v_{\rm a}}} \cdot \underline{E_{0vv}^{X} Q_{0vv}^{X}} \\ & - \underline{P_0^{v_{\rm b}}} \cdot \underline{E_{v0v}^{X} Q_{v0v}^{X}} + \overline{P_0^{v_{\rm a}}} \cdot \overline{P_0^{v_{\rm b}}} \cdot \overline{E_{00v}^{X} Q_{00v}^{X}} \\ & - \underline{P_0^{v_{\rm c}}} \cdot \underline{E_{vv0}^{X} Q_{vv0}^{X}} + \overline{P_0^{v_{\rm b}}} \cdot \overline{P_0^{v_{\rm c}}} \cdot \overline{E_{v00}^{X} Q_{v00}^{X}} \\ & + \overline{P_0^{v_{\rm a}}} \cdot \overline{P_0^{v_{\rm c}}} \cdot \overline{E_{0v0}^{X} Q_{0v0}^{X}} - \underline{P_0^{v_{\rm a}}} \cdot \underline{P_0^{v_{\rm b}}} \cdot \underline{P_0^{v_{\rm c}}} \cdot \underline{E_{000}^{X} Q_{000}^{X}}), \end{aligned}$$

where $E_{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}^{Z} Q_{\gamma_{\rm a}\gamma_{\rm b}\gamma_{\rm c}}^{Z} (\gamma_{\rm a},\gamma_{\rm b},\gamma_{\rm c} \in \{v,0\})$ are the error rate of single-photon pulse of untagged pulses when Alice's, Bob's, and Charlie's intensity settings are $\gamma_{\rm a},\gamma_{\rm b},\gamma_{\rm c}$ respectively, and their bounds can be estimated from Eq. (4). $\overline{P_0^{v_s}}$ and $\underline{P_0^{v_s}}(s = {\rm a,b,c})$ are defined by Eq. (2).

4.3. Secret key rate

We analyze the behavior of the secret key rate of MDI-QCC with an untrusted source such that

$$R \ge (1-\Delta_{\rm a}-\varepsilon_{\rm a})(1-\Delta_{\rm b}-\varepsilon_{\rm b})(1-\Delta_{\rm c}-\varepsilon_{\rm c}) \times \underline{Q_{111}^{Z}}(1-H_2(\overline{e_{111}^{X}})) + \underline{Q_{v}^{Z}} - H_2(E_{uuu}^{Z}) f Q_{uuu}^{Z},$$

where Q_{uuu}^{Z} (E_{uuu}^{Z}) is the gain (the total quantum bit error rate) of Z basis when Alice, Bob, and Charlie use signal states, which can be directly obtained from the experimental results; $\underline{Q_{v}^{Z}} = \underline{P_0^{u}(m_{\rm a})} \cdot \underline{Q_{0uu}^{Z}}$ is the lower bound of the gain that Alice sends out vacuum state in Z basis, given that Alice, Bob, and Charlie all send states in untagged pulses; $\underline{Q_{111}^{Z}}$ and $\overline{e_{111}^{X}}$ are the lower bound of the gain in the Z basis and the upper bound of the error rate in the X basis, given that Alice, Bob, and Charlie all send single-photon states in untagged pulses.

5. Numerical simulation

By assuming a fiber-based channel model, we numerically show the performance of our protocol in the asymptotic case in comparison with Ref. [43] (the case with trusted sources). The experimental parameters for simulation are listed in Table 1.

Table 1. List of experimental parameters for simulations: $\eta_{\rm d}$ and Y_0 are the detection efficiency and the dark-count rate of David's single photon detectors, $e_{\rm d}$ represents the overall misalignment-error probability of the system,[43] $\eta_{\rm ID}$ and $\sigma_{\rm ID}$ are the the efficiency and the noise of intensity detector, q is the beam-splitter ratio,[29] α is the loss coefficient of the fiber, and f is the error-correction efficiency.

$\eta_{\rm d}$	Y_0	$\eta_{\rm ID}$	$\sigma_{\rm ID}$	$e_{\rm d}$	f	q	α
40%	3×1^{-7}	0.7	6.55×10^{4}	1.5%	1.16	0.01	0.20db/km

In Fig. 2, we consider the imperfections of the intensity monitor in implementation[29] and present the numerical simulation of secret-key rates with different values of $M_{\rm d}$, which is the average photon number per pulse at the source in the middle node. In the simulation, we consider two decoy state (weak+vacuum) protocols. Specifically, the intensity of one decoy state is 0.01 and the other decoy state is a vacuum state, while the signal state is optimized for different distances. Since $\delta_s(s = {\rm a,b,c})$ can significantly affect the performance of the protocol,[46,47] we optimize δ_s $(s = {\rm a,b,c})$ for different distances.

From the simulation results, we can find that as for the secret key rates, our protocol (the MDI-QCC with an untrusted source) and the case with trusted sources[43] are neck and neck at short distances. However, at long distances the secret key rates of our protocol reduce significantly. The reason is that due to the bi-directional structure, bright pulses sent by David will suffer the whole channel loss. This means that as the distances increase, lower photons per pulse can arrive at Alice's, Bob's, and Charlie's labs, which leads to the increase of Δ_s $(s = {\rm a,b,c})$.

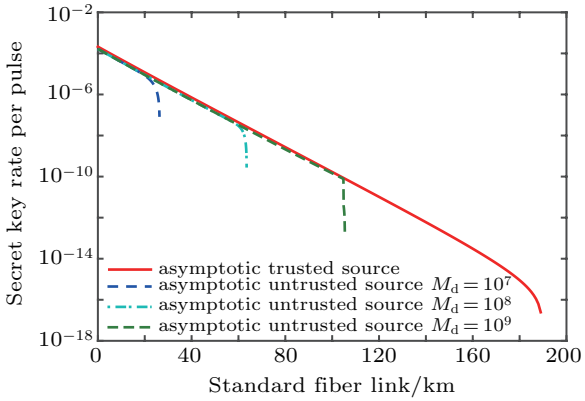

Fig. 2. (color online) Secret key rate versus fiber length with different values of M_d. The red dashed curve denotes the asymptotic secret key rate with trusted source in Ref. [43]. At short distance, the asymptotic key rates for the two cases (with trusted and untrusted sources) almost overlap. With $M_d = 10^9$ and considering the imperfections of intensity detector, MDI-QCC with an untrusted source can achieve the nonzero asymptotic secret key rate in long distance approximating to 105 km.

Moreover, from Eqs. (3) and (4), we know the estimation of the gain of the untagged pulses is sensitive to the value of $\Delta_s(s = \mathrm{a,b,c})$ which affects the performance directly. This influence is much greater than that of Refs. [29], [46], and [47]. Because MDI-QCC is a multi-party protocol, the influence on Δ_s $(s = \mathrm{a,b,c})$ will affect the parameter estimating of the untagged pulses together. In other words, the influence on each party accumulates.

6. Conclusion

We extend the framework of MDI-QKD with an untrusted source[29] to MDI-QCC and give the rigorous security analysis of MDI-QCC with an untrusted source. The protocol of MDI-QCC with an untrusted source utilizes the bi-directional structure and can certainly mitigate the experimental complexity of MDI-QCC. What is more, inspired by the security analysis for plug & play QKD,[46,47] we clearly provide rigorous analytical method for parameters' estimation based on the actual photon number distribution of user's output pulses. With simple modifications, our analytical method can be applied to not only MDI-QKD with an untrusted source, but also arbitrary multi-party communication protocol with an untrusted source. To some extent, our work can be an important step towards practical application for quantum networks.

The numerical simulation results show that we can achieve the nonzero asymptotic secret key rate over reasonable distances, and the secret key rates for our protocol and the case with trusted source almost overlap at short distances. Importantly, our framework and security analysis can be extended to arbitrary multi-party communication not merely confined to three parties and can also be applied to MDI-QSS[43] protocol and MDI-QCC protocol using W-state.[44] To make the protocol of MDI-QCC with an untrusted source more practical, it is necessary to settle the remaining practical issues, such as the source flaws and the imperfections in the electronics of the classical intensity detector.

Appendix A: Derivation of a lower bound of Q^Z_{111}

By performing the measurements for signal, decoy, and vacuum states, the gain of untagged pulses can be denoted as

$$\begin{aligned}
Q^Z_{uuu} &= \sum_{m_\mathrm{a},m_\mathrm{b},m_\mathrm{c}} \sum_{n_\mathrm{a},n_\mathrm{b},n_\mathrm{c}} P_{\mathrm{in}}(m_\mathrm{a}m_\mathrm{b}m_\mathrm{c}) P^u_{n_\mathrm{a}}(m_\mathrm{a}) P^u_{n_\mathrm{b}}(m_\mathrm{b}) \\
&\quad \times P^u_{n_\mathrm{c}}(m_\mathrm{c}) Y_{m_{\mathrm{a,b,c}} n_{\mathrm{a,b,c}}}, \\
Q^Z_{vvv} &= \sum_{m_\mathrm{a},m_\mathrm{b},m_\mathrm{c}} \sum_{n_\mathrm{a},n_\mathrm{b},n_\mathrm{c}} P_{\mathrm{in}}(m_\mathrm{a}m_\mathrm{b}m_\mathrm{c}) P^v_{n_\mathrm{a}}(m_\mathrm{a}) \\
&\quad \times P^v_{n_\mathrm{b}}(m_\mathrm{b}) P^v_{n_\mathrm{c}}(m_\mathrm{c}) Y_{m_{\mathrm{a,b,c}} n_{\mathrm{a,b,c}}}, \\
Q^Z_{000} &= \sum_{m_\mathrm{a},m_\mathrm{b},m_\mathrm{c}} P_{\mathrm{in}}(m_\mathrm{a}m_\mathrm{b}m_\mathrm{c}) Y_{m_{\mathrm{a,b,c}} 0_{\mathrm{a,b,c}}},
\end{aligned} \tag{A1}$$

where $m_s \in [(1-\delta_s)M_s, (1+\delta_s)M_s]$, and $n_s \in [0, (1+\delta_s)M_s]$ $(s = \mathrm{a,b,c})$. When Alice, Bob, and Charlie choose the signal state simultaneously, Q^Z_{111} can be written as

$$\begin{aligned}
Q^Z_{111} &= \sum_{m_\mathrm{a},m_\mathrm{b},m_\mathrm{c}} P_{\mathrm{in}}(m_\mathrm{a}m_\mathrm{b}m_\mathrm{c}) P^u_1(m_\mathrm{a}) P^u_1(m_\mathrm{b}) P^u_1(m_\mathrm{c}) Y_{m_{\mathrm{a,b,c}} 111} \\
&\geq \underline{P^{u_\mathrm{a}}_1} \cdot \underline{P^{u_\mathrm{b}}_1} \cdot \underline{P^{u_\mathrm{c}}_1} \sum_{m_\mathrm{a},m_\mathrm{b},m_\mathrm{c}} P_{\mathrm{in}}(m_\mathrm{a}m_\mathrm{b}m_\mathrm{c}) Y_{m_{\mathrm{a,b,c}} 111} \\
&= \underline{P^{uuu}_{111}} \sum_{m_\mathrm{a},m_\mathrm{b},m_\mathrm{c}} P_{\mathrm{in}}(m_\mathrm{a}m_\mathrm{b}m_\mathrm{c}) Y_{m_{\mathrm{a,b,c}} 111} \\
&= \underline{P^{uuu}_{111}} V_{111}.
\end{aligned}$$

Thus, in order to get a lower bound of Q^Z_{111} , we should derive the lower bound of V_{111}. Combining Eqs. (A1), (2), and (11), we can get

$$\begin{aligned}
&Q^Z_{uuu} \overline{P^{vvv}_{222}} - Q^Z_{vvv} \underline{P^{uuu}_{222}} \\
&= \sum_{m_\mathrm{a},m_\mathrm{b},m_\mathrm{c}} P_{\mathrm{in}}(m_\mathrm{a}m_\mathrm{b}m_\mathrm{c}) \\
&\quad \times \sum_{n_\mathrm{a},n_\mathrm{b},n_\mathrm{c}=0}^{(1+\delta_s)M_s} (P^u_{n_\mathrm{a}}(m_\mathrm{a}) P^u_{n_\mathrm{b}}(m_\mathrm{b}) P^u_{n_\mathrm{c}}(m_\mathrm{c}) \overline{P^{vvv}_{222}} \\
&\quad - P^v_{n_\mathrm{a}}(m_\mathrm{a}) P^v_{n_\mathrm{b}}(m_\mathrm{b}) P^v_{n_\mathrm{c}}(m_\mathrm{c}) \underline{P^{uuu}_{222}}) Y_{m_{\mathrm{a,b,c}} n_{\mathrm{a,b,c}}} \\
&\geq \sum_{m_\mathrm{a},m_\mathrm{b},m_\mathrm{c}} P_{\mathrm{in}}(m_\mathrm{a}m_\mathrm{b}m_\mathrm{c}) \sum_{n_\mathrm{a},n_\mathrm{b},n_\mathrm{c}=0}^{(1+\delta_s)M_s} (\underline{P^u_{n_\mathrm{a}}} \cdot \underline{P^u_{n_\mathrm{b}}} \cdot \underline{P^u_{n_\mathrm{c}}} \overline{P^{vvv}_{222}} \\
&\quad - \overline{P^v_{n_\mathrm{a}}} \cdot \overline{P^v_{n_\mathrm{a}}} \cdot \overline{P^v_{n_\mathrm{a}}} \cdot \underline{P^{uuu}_{222}}) Y_{m_{\mathrm{a,b,c}} n_{\mathrm{a,b,c}}} \\
&= \sum_{n_\mathrm{a},n_\mathrm{b},n_\mathrm{c}=0}^{(1+\delta_s)M_s} \left(\underline{P^{uuu}_{n_\mathrm{a}n_\mathrm{b}n_\mathrm{c}}} \overline{P^{vvv}_{222}} - \overline{P^{vvv}_{n_\mathrm{a}n_\mathrm{b}n_\mathrm{c}}} \underline{P^{uuu}_{222}} \right) \\
&\quad \times \sum_{m_\mathrm{a},m_\mathrm{b},m_\mathrm{c}} P_{\mathrm{in}}(m_\mathrm{a}m_\mathrm{b}m_\mathrm{c}) Y_{m_{\mathrm{a,b,c}} n_{\mathrm{a,b,c}}} \\
&= r_0 Q^Z_{000} + r_1 V_{111} + \sum_{n_\mathrm{a},n_\mathrm{b},n_\mathrm{c}=3}^{(1-\delta_s)M_s} r_{n_\mathrm{a}n_\mathrm{b}n_\mathrm{c}} V_{n_\mathrm{a}n_\mathrm{b}n_\mathrm{c}} + r_3,
\end{aligned}$$

where

$$r_0 = \underline{P^{uuu}_{000}} \overline{P^{vvv}_{222}} - \overline{P^{vvv}_{000}} \underline{P^{uuu}_{222}}, \tag{A2}$$

$$r_1 = \underline{P^{uuu}_{111}} \overline{P^{vvv}_{222}} - \overline{P^{vvv}_{111}} \underline{P^{uuu}_{222}}, \tag{A3}$$

$$r_{n_a n_b n_c} = \underline{P^{uuu}_{n_a n_b n_c}}\,\overline{P^{vvv}_{222}} - \overline{P^{vvv}_{n_a n_b n_c}}\,\underline{P^{uuu}_{222}}, \tag{A4}$$

$$r_3 = -\sum_{n_a,n_b,n_c=(1-\delta_s)M_s+1}^{(1+\delta_s)M_s} \overline{P^{vvv}_{n_a n_b n_c}}\,\underline{P^{uuu}_{222}} V_{n_a n_b n_c}, \tag{A5}$$

$$V_{n_a n_b n_c} = \sum_{m_a,m_b,m_c} P_{in}(m_a m_b m_c) Y_{m_{a,b,c} n_{a,b,c}}. \tag{A6}$$

If we prove that $r_0 < 0$, $r_1 < 0$, and $r_{n_a n_b n_c} > 0$, we can get the lower bound of V_{111}, that is

$$V_{111} \geq \frac{Q^Z_{vvv}\underline{P^{uuu}_{222}} - Q^Z_{uuu}\overline{P^{vvv}_{222}} + r_0 Q^Z_{000} + \sum_{n_a,n_b,n_c=3}^{(1-\delta_s)M_s} r_{n_a n_b n_c} V_{n_a n_b n_c} + r_3}{-r_1} > \frac{\underline{Q^Z_{vvv}}\cdot\underline{P^{uuu}_{222}} - \overline{Q^Z_{uuu}}\cdot\overline{P^{vvv}_{222}} + r_0 Q^Z_{000} + r_3}{-r_1}. \tag{A7}$$

Then, if $r_3 \sim 0$, Eq. (A7) can be written as

$$V_{111} > \frac{\underline{Q^Z_{vvv}}\cdot\underline{P^{uuu}_{222}} - \overline{Q^Z_{uuu}}\cdot\overline{P^{vvv}_{222}} + r_0 Q^Z_{000}}{-r_1}.$$

Proof of $r_0 < 0$ and $r_1 < 0$

Corollary 1 Under Condition 1, $r_0 < 0$ and $r_1 < 0$.

Condition 1:

$$\frac{\lambda_a^u\lambda_b^u\lambda_c^u}{\lambda_a^v\lambda_b^v\lambda_c^v} > \frac{((1+\delta_a)M_a-1)((1+\delta_b)M_b-1)((1+\delta_c)M_c-1)}{((1-\delta_a)M_a-1)((1-\delta_b)M_b-1)((1-\delta_c)M_c-1)}.$$

Proof Plugging Eqs. (2) and (11) into Eq. (A2), r_0 can be developed as

$$\begin{aligned}
r_0 =\ & (1-\lambda_a^v q)^{(1-\delta_a)M_a}(1-\lambda_b^v q)^{(1-\delta_b)M_b} \\
& \times (1-\lambda_c^v q)^{(1-\delta_c)M_c}(1-\lambda_a^u q)^{(1-\delta_a)M_a-2} \\
& \times (1-\lambda_b^u q)^{(1-\delta_b)M_b-2}(1-\lambda_c^u q)^{(1-\delta_c)M_c-2} \\
& \times [(1-\lambda_a^v q)^{2\delta_a M_a-2}(1-\lambda_b^v q)^{2\delta_b M_b-2}(1-\lambda_c^v q)^{2\delta_c M_c-2} \\
& \times (1-\lambda_a^u q)^{2\delta_a M_a+2}(1-\lambda_b^u q)^{2\delta_b M_b+2} \\
& \times (1-\lambda_c^u q)^{2\delta_c M_c+2} C^2_{(1+\delta_a)M_a} C^2_{(1+\delta_b)M_b} \\
& \times C^2_{(1+\delta_c)M_c}(\lambda_a^v\lambda_b^v\lambda_c^v)^2 q^6 - C^2_{(1-\delta_a)M_a} \\
& \times C^2_{(1-\delta_b)M_b} C^2_{(1-\delta_c)M_c}(\lambda_a^u\lambda_b^u\lambda_c^u)^2 q^6] \\
< & C^2_{(1+\delta_a)M_a} C^2_{(1+\delta_b)M_b} C^2_{(1+\delta_c)M_c}(\lambda_a^v\lambda_b^v\lambda_c^v)^2 q^6 \\
& - C^2_{(1-\delta_a)M_a} C^2_{(1-\delta_b)M_b} C^2_{(1-\delta_c)M_c}(\lambda_a^u\lambda_b^u\lambda_c^u)^2 q^6 \\
< & 0,
\end{aligned}$$

where C_n^r is the combination formula. Then under Condition 1, we can find $r_0 < 0$.

Plugging Eqs. (2) and (11) into Eq. (A3), r_1 can be developed as

$$\begin{aligned}
r_1 = & (1-\lambda_a^u q)^{(1-\delta_a)M_a-2}(1-\lambda_b^u q)^{(1-\delta_b)M_b-2} \\
& \times (1-\lambda_c^u q)^{(1-\delta_c)M_c-2}(1-\lambda_a^v q)^{(1+\delta_a)M_a-2} \\
& \times (1-\lambda_b^v q)^{(1+\delta_b)M_b-2}(1-\lambda_c^v q)^{(1+\delta_c)M_c-2} \\
& \times (\lambda_a^u\lambda_b^u\lambda_c^u\lambda_a^v\lambda_b^v\lambda_c^v M_a M_b M_c q^9) \\
& \times [(1-\delta_a)(1-\delta_b)(1-\delta_c)(1-\lambda_a^u q) \\
& \times (1-\lambda_b^u q)(1-\lambda_c^u q)\lambda_a^v\lambda_b^v\lambda_c^v C^2_{(1+\delta_a)M_a} \\
& \times C^2_{(1+\delta_b)M_b} C^2_{(1+\delta_c)M_c} - (1+\delta_a) \\
& \times (1+\delta_b)(1+\delta_c)(1-\lambda_a^v q)(1-\lambda_b^v q)(1-\lambda_c^v q) \\
& \times \lambda_a^u\lambda_b^u\lambda_c^u C^2_{(1-\delta_a)M_a} C^2_{(1-\delta_b)M_b} C^2_{(1-\delta_c)M_c}] \\
= & (1-\lambda_a^u q)^{(1-\delta_a)M_a-2}(1-\lambda_b^u q)^{(1-\delta_b)M_b-2} \\
& \times (1-\lambda_c^u q)^{(1-\delta_c)M_c-2}(1-\lambda_a^v q)^{(1+\delta_a)M_a-2} \\
& \times (1-\lambda_b^v q)^{(1+\delta_b)M_b-2}(1-\lambda_c^v q)^{(1+\delta_c)M_c-2} \\
& \times (\lambda_a^u\lambda_b^u\lambda_c^u\lambda_a^v\lambda_b^v\lambda_c^v {M_a}^2 {M_b}^2 {M_c}^2 q^9) \\
& \times \frac{1}{8}\left(1-\delta_a^2\right)\left(1-\delta_b^2\right)\left(1-\delta_c^2\right)[(1-\lambda_a^u q)(1-\lambda_b^u q) \\
& \times (1-\lambda_c^u q)\lambda_a^v\lambda_b^v\lambda_c^v((1+\delta_a)M_a-1)((1+\delta_b)M_b-1) \\
& \times ((1+\delta_c)M_c-1) - (1-\lambda_a^v q)(1-\lambda_b^v q)(1-\lambda_c^v q) \\
& \times ((1-\delta_a)M_a-1)((1-\delta_b)M_b-1) \\
& \times ((1-\delta_c)M_c-1)\lambda_a^u\lambda_b^u\lambda_c^u].
\end{aligned} \tag{A8}$$

Under Condition 1, we can find

$$(1-\lambda_a^u q)(1-\lambda_b^u q)(1-\lambda_c^u q) < (1-\lambda_a^v q)(1-\lambda_b^v q)(1-\lambda_c^v q).$$

Then, Eq. (A8) can be developed as

$$\begin{aligned}
r_1 < & (1-\lambda_a^u q)^{(1-\delta_a)M_a-2}(1-\lambda_b^u q)^{(1-\delta_b)M_b-2} \\
& \times (1-\lambda_c^u q)^{(1-\delta_c)M_c-2}(1-\lambda_a^v q)^{(1+\delta_a)M_a-2} \\
& \times (1-\lambda_b^v q)^{(1+\delta_b)M_b-2}(1-\lambda_c^v q)^{(1+\delta_c)M_c-2} \\
& \times (\lambda_a^u\lambda_b^u\lambda_c^u\lambda_a^v\lambda_b^v\lambda_c^v {M_a}^2 {M_b}^2 {M_c}^2 q^9) \\
& \times \frac{1}{8}\left(1-\delta_a^2\right)\left(1-\delta_b^2\right)\left(1-\delta_c^2\right)(1-\lambda_a^v q) \\
& \times (1-\lambda_b^v q)(1-\lambda_c^v q)[\lambda_a^v\lambda_b^v\lambda_c^v((1+\delta_a)M_a-1) \\
& \times ((1+\delta_b)M_b-1)((1+\delta_c)M_c-1) - ((1-\delta_a)M_a-1) \\
& \times ((1-\delta_b)M_b-1)((1-\delta_c)M_c-1)\lambda_a^u\lambda_b^u\lambda_c^u].
\end{aligned}$$

Under Condition 1, we can easily find $r_1 < 0$.

Proof of $r_3 \sim 0$ and $r_{n_a n_b n_c} > 0$

Corollary 2 r_3 is in the order of $O(\frac{1}{M_a!M_b!M_c!})$.

Proof Since $0 \leq V_{n_a n_b n_c} \leq 1$, r_3 (Eq. A5) can be developed as

$$r_3 \geq -\sum_{n_a,n_b,n_c=(1-\delta_s)M_s+1}^{(1+\delta_s)M_s} \overline{P^{vvv}_{n_a n_b n_c}}\,\underline{P^{uuu}_{222}}. \tag{A9}$$

With Eqs. (2) and (11), we can find

$$\overline{P^{vvv}_{n_a n_b n_c}} < \overline{P^v_{(1-\delta_a)M_a+1}(m_a)}\cdot\overline{P^v_{(1-\delta_b)M_b+1}(m_b)}\cdot\overline{P^v_{(1-\delta_c)M_c+1}(m_c)}.$$

Then, equation (A9) can be developed as

$$\begin{aligned} r_3 \geq & -8\delta_{\rm a}\delta_{\rm b}\delta_{\rm c}M_{\rm a}M_{\rm b}M_{\rm c}\cdot\overline{P^{v}_{(1-\delta_{\rm a})M_{\rm a}+1}(m_{\rm a})} \\ & \times\overline{P^{v}_{(1-\delta_{\rm b})M_{\rm b}+1}(m_{\rm b})}\cdot\overline{P^{v}_{(1-\delta_{\rm c})M_{\rm c}+1}(m_{\rm c})}\underline{P^{uuu}_{222}} \\ = & -8\delta_{\rm a}\delta_{\rm b}\delta_{\rm c}M_{\rm a}M_{\rm b}M_{\rm c}\cdot\frac{1}{((1-\delta_{\rm a})M_{\rm a}+1)!} \\ & \times\frac{1}{((1-\delta_{\rm b})M_{\rm b}+1)!}\cdot\frac{1}{((1-\delta_{\rm c})M_{\rm c}+1)!} \\ & \times(1-\lambda_{\rm a}^{v})^{2\delta_{\rm a}M_{\rm a}-1}(1-\lambda_{\rm b}^{v})^{2\delta_{\rm b}M_{\rm b}-1}(1-\lambda_{\rm c}^{v})^{2\delta_{\rm c}M_{\rm c}-1}\underline{P^{uuu}_{222}} \\ & \times\prod_{i=0}^{(1-\delta_{\rm a})M_{\rm a}}[((1+\delta_{\rm a})M_{\rm a}-i)\lambda_{\rm a}^{v}q] \\ & \times\prod_{j=0}^{(1-\delta_{\rm b})M_{\rm b}}[((1+\delta_{\rm b})M_{\rm b}-j)\lambda_{\rm b}^{v}q] \\ & \times\prod_{k=0}^{(1-\delta_{\rm c})M_{\rm c}}[((1+\delta_{\rm c})M_{\rm c}-k)\lambda_{\rm c}^{v}q]. \end{aligned} \tag{A10}$$

Since $[((1+\delta_s)M_s-i)\lambda_s^v q]<1$, where $i\in[0,(1-\delta_s)M_s](s={\rm a,b,c})$, Eq. (A10) can be developed as

$$\begin{aligned} r_3 > & -8\delta_{\rm a}\delta_{\rm b}\delta_{\rm c}M_{\rm a}M_{\rm b}M_{\rm c}\cdot\frac{1}{((1-\delta_{\rm a})M_{\rm a}+1)!} \\ & \times\frac{1}{((1-\delta_{\rm b})M_{\rm b}+1)!}\cdot\frac{1}{((1-\delta_{\rm c})M_{\rm c}+1)!} \\ & \times(1-\lambda_{\rm a}^{v})^{2\delta_{\rm a}M_{\rm a}-1}(1-\lambda_{\rm b}^{v})^{2\delta_{\rm b}M_{\rm b}-1}(1-\lambda_{\rm c}^{v})^{2\delta_{\rm c}M_{\rm c}-1}\underline{P^{uuu}_{222}}. \end{aligned}$$

Therefore, we have that r_3 is in the order of $O(\frac{1}{M_{\rm a}!M_{\rm b}!M_{\rm c}!})$, and $r_3\sim 0$.

Corollary 3 Under Condition 2, $r_{n_{\rm a}n_{\rm b}n_{\rm c}}>0$.

Condition 2:

$$\frac{\lambda_{\rm a}^{u}\lambda_{\rm b}^{u}\lambda_{\rm c}^{u}}{\lambda_{\rm a}^{v}\lambda_{\rm b}^{v}\lambda_{\rm c}^{v}} > C_{(1+\delta_{\rm a})M_{\rm a}-2}^{2\delta_{\rm a}M_{\rm a}}{}^{\frac{1}{(1-\delta_{\rm a})M_{\rm a}-2}}C_{(1+\delta_{\rm b})M_{\rm b}-2}^{2\delta_{\rm b}M_{\rm b}}{}^{\frac{1}{(1-\delta_{\rm b})M_{\rm b}-2}} \times C_{(1+\delta_{\rm c})M_{\rm c}-2}^{2\delta_{\rm c}M_{\rm c}}{}^{\frac{1}{(1-\delta_{\rm c})M_{\rm c}-2}}.$$

Proof Plugging Eqs. (2) and (11) into Eq. (A4), $r_{n_{\rm a}n_{\rm b}n_{\rm c}}$ can be developed as

$$\begin{aligned} r_{n_{\rm a}n_{\rm b}n_{\rm c}} = & (\lambda_{\rm a}^{u}\lambda_{\rm b}^{u}\lambda_{\rm c}^{u}\lambda_{\rm a}^{v}\lambda_{\rm b}^{v}\lambda_{\rm c}^{v}q^{6})^{2}(1-\lambda_{\rm a}^{u}q)^{(1-\delta_{\rm a})M_{\rm a}-n_{\rm a}} \\ & \times(1-\lambda_{\rm b}^{u}q)^{(1-\delta_{\rm b})M_{\rm b}-n_{\rm b}}(1-\lambda_{\rm c}^{u}q)^{(1-\delta_{\rm c})M_{\rm c}-n_{\rm c}} \\ & \times(1-\lambda_{\rm a}^{v}q)^{(1+\delta_{\rm a})M_{\rm a}-n_{\rm a}}(1-\lambda_{\rm b}^{v}q)^{(1+\delta_{\rm b})M_{\rm b}-n_{\rm b}} \\ & \times(1-\lambda_{\rm c}^{v}q)^{(1+\delta_{\rm c})M_{\rm c}-n_{\rm c}} \\ & \times\frac{(1-\delta_{\rm a})M_{\rm a}!(1+\delta_{\rm a})M_{\rm a}!(1-\delta_{\rm b})M_{\rm b}!(1+\delta_{\rm b})M_{\rm b}!}{4n_{\rm a}!n_{\rm b}!} \\ & \times\frac{(1-\delta_{\rm c})M_{\rm c}!(1+\delta_{\rm c})M_{\rm c}!}{2n_{\rm c}!}[Z_1-Z_2], \end{aligned}$$

where

$$Z_1=\frac{(\lambda_{\rm a}^{u}q)^{n_{\rm a}-2}(1-\lambda_{\rm a}^{v}q)^{n_{\rm a}-2}(\lambda_{\rm b}^{u}q)^{n_{\rm b}-2}(1-\lambda_{\rm b}^{v}q)^{n_{\rm b}-2}}{((1+\delta_{\rm a})M_{\rm a}-2)!((1-\delta_{\rm a})M_{\rm a}-n_{\rm a})!((1+\delta_{\rm b})M_{\rm b}-2)!((1-\delta_{\rm b})M_{\rm b}-n_{\rm b})!}\frac{(\lambda_{\rm c}^{u}q)^{n_{\rm c}-2}(1-\lambda_{\rm c}^{v}q)^{n_{\rm c}-2}}{((1+\delta_{\rm c})M_{\rm c}-2)!((1-\delta_{\rm c})M_{\rm c}-n_{\rm c})!},$$

and

$$Z_2=\frac{(\lambda_{\rm a}^{v}q)^{n_{\rm a}-2}(1-\lambda_{\rm a}^{u}q)^{n_{\rm a}-2}(\lambda_{\rm b}^{v}q)^{n_{\rm b}-2}(1-\lambda_{\rm b}^{u}q)^{n_{\rm b}-2}}{((1-\delta_{\rm a})M_{\rm a}-2)!((1+\delta_{\rm a})M_{\rm a}-n_{\rm a})!((1-\delta_{\rm b})M_{\rm b}-2)!((1+\delta_{\rm b})M_{\rm b}-n_{\rm b})!}\frac{(\lambda_{\rm c}^{v}q)^{n_{\rm c}-2}(1-\lambda_{\rm c}^{u}q)^{n_{\rm c}-2}}{((1-\delta_{\rm c})M_{\rm c}-2)!((1+\delta_{\rm c})M_{\rm c}-n_{\rm c})!}.$$

It is easy to find that $Z_1>0$ and $Z_2>0$. So in order to prove $r_{n_{\rm a}n_{\rm b}n_{\rm c}}>0$, we need to show $Z_1/Z_2>1$. Z_1/Z_2 can be written as

$$\begin{aligned} \frac{Z_1}{Z_2} = & \prod_{i=3}^{n_{\rm a}}\left[\frac{(1-\delta_{\rm a})M_{\rm a}-i+1}{(1+\delta_{\rm a})M_{\rm a}-i+1}\cdot\frac{\lambda_{\rm a}^{u}(1-\lambda_{\rm a}^{v})}{\lambda_{\rm a}^{v}(1-\lambda_{\rm a}^{u})}\right] \\ & \times\prod_{j=3}^{n_{\rm b}}\left[\frac{(1-\delta_{\rm b})M_{\rm b}-j+1}{(1+\delta_{\rm b})M_{\rm b}-j+1}\cdot\frac{\lambda_{\rm b}^{u}(1-\lambda_{\rm b}^{v})}{\lambda_{\rm b}^{v}(1-\lambda_{\rm b}^{u})}\right] \\ & \times\prod_{k=3}^{n_{\rm b}}\left[\frac{(1-\delta_{\rm c})M_{\rm c}-k+1}{(1+\delta_{\rm c})M_{\rm c}-k+1}\cdot\frac{\lambda_{\rm c}^{u}(1-\lambda_{\rm c}^{v})}{\lambda_{\rm c}^{v}(1-\lambda_{\rm c}^{u})}\right]. \end{aligned}$$

Let

$$f(i)=\frac{(1-\delta_s)M_s-i+1}{(1+\delta_s)M_s-i+1}\cdot\frac{\lambda_s^{u}(1-\lambda_s^{v})}{\lambda_s^{v}(1-\lambda_s^{u})},\ i\in[3,n_s]\ (s={\rm a,b,c}).$$

Since $f(i)>0$ and decreases as i increases, there is a positive integer i_0 making $f(i)>1, i<i_0$ and $f(i)<1, i\geq i_0$ stand. So if $n_{\rm a},n_{\rm b},n_{\rm c}<i_0$, $Z_1/Z_2>1$ obviously holds. If $n_{\rm a},n_{\rm b},n_{\rm c}\geq i_0$, we can find $(1-\delta_s)M_s\geq n_{\rm a},n_{\rm b},n_{\rm c}\geq i_0(s={\rm a,b,c})$. So in this case, Z_1/Z_2 can be developed as

$$\begin{aligned} Z_1/Z_2 \geq & \prod_{i=3}^{(1-\delta_{\rm a})M_{\rm a}}\left[\frac{(1-\delta_{\rm a})M_{\rm a}-i+1}{(1+\delta_{\rm a})M_{\rm a}-i+1}\cdot\frac{\lambda_{\rm a}^{u}(1-\lambda_{\rm a}^{v})}{\lambda_{\rm a}^{v}(1-\lambda_{\rm a}^{u})}\right] \\ & \times\prod_{j=3}^{(1-\delta_{\rm b})M_{\rm b}}\left[\frac{(1-\delta_{\rm b})M_{\rm b}-j+1}{(1+\delta_{\rm b})M_{\rm b}-j+1}\cdot\frac{\lambda_{\rm b}^{u}(1-\lambda_{\rm b}^{v})}{\lambda_{\rm b}^{v}(1-\lambda_{\rm b}^{u})}\right] \\ & \times\prod_{k=3}^{(1-\delta_{\rm c})M_{\rm c}}\left[\frac{(1-\delta_{\rm c})M_{\rm c}-k+1}{(1+\delta_{\rm c})M_{\rm c}-k+1}\cdot\frac{\lambda_{\rm c}^{u}(1-\lambda_{\rm c}^{v})}{\lambda_{\rm c}^{v}(1-\lambda_{\rm c}^{u})}\right] \\ = & \frac{1}{C_{(1+\delta_{\rm a})M_{\rm a}-2}^{2\delta_{\rm a}M_{\rm a}}}\left(\frac{\lambda_{\rm a}^{u}(1-\lambda_{\rm a}^{v})}{\lambda_{\rm a}^{v}(1-\lambda_{\rm a}^{u})}\right)^{(1+\delta_{\rm a})M_{\rm a}-2} \\ & \times\frac{1}{C_{(1+\delta_{\rm b})M_{\rm b}-2}^{2\delta_{\rm b}M_{\rm b}}}\left(\frac{\lambda_{\rm b}^{u}(1-\lambda_{\rm b}^{v})}{\lambda_{\rm b}^{v}(1-\lambda_{\rm b}^{u})}\right)^{(1+\delta_{\rm b})M_{\rm b}-2} \\ & \times\frac{1}{C_{(1+\delta_{\rm c})M_{\rm c}-2}^{2\delta_{\rm c}M_{\rm c}}}\left(\frac{\lambda_{\rm c}^{u}(1-\lambda_{\rm c}^{v})}{\lambda_{\rm c}^{v}(1-\lambda_{\rm c}^{u})}\right)^{(1+\delta_{\rm c})M_{\rm c}-2}. \end{aligned}$$

Under Condition 2, we can find that $Z_1/Z_2>1$. So far, $r_{n_{\rm a}n_{\rm b}n_{\rm c}}>0$ has been proved.

However, when M_a, M_b, M_c is large, the computation of Condition 2 is difficult. So we give a simpler condition denoted as Condition 3 with Stirling's approximation ($n^{n+1/2}\,e^{-n} < n! < n^{n+1/2}\,e^{-n+1}$).

Condition 3:

$$\frac{\lambda_a^u\lambda_b^u\lambda_c^u}{\lambda_a^v\lambda_b^v\lambda_c^v} > \frac{((1+\delta_a)M_a-2)((1+\delta_b)M_b-2)((1+\delta_c)M_c-2)}{((1-\delta_a)M_a-2)((1-\delta_b)M_b-2)((1-\delta_c)M_c-2)} \times K_1K_2\cdot K_3,$$

where

$$K_1 = \left(\frac{e\cdot((1+\delta_a)M_a-2)^{2\delta_aM_a+\frac{1}{2}}}{(2\delta_aM_a)^{2\delta_aM_a+\frac{1}{2}}((1-\delta_a)M_a-2)^{\frac{1}{2}}}\right)^{\frac{1}{(1-\delta_a)M_a-2}},$$

$$K_2 = \left(\frac{e\cdot((1+\delta_b)M_b-2)^{2\delta_bM_b+\frac{1}{2}}}{(2\delta_bM_b)^{2\delta_bM_b+\frac{1}{2}}((1-\delta_b)M_b-2)^{\frac{1}{2}}}\right)^{\frac{1}{(1-\delta_b)M_b-2}},$$

$$K_3 = \left(\frac{e\cdot((1+\delta_c)M_c-2)^{2\delta_cM_c+\frac{1}{2}}}{(2\delta_cM_c)^{2\delta_cM_c+\frac{1}{2}}((1-\delta_c)M_c-2)^{\frac{1}{2}}}\right)^{\frac{1}{(1-\delta_c)M_c-2}}.$$

It should be noted that Condition 3 is stronger than Condition 2, and Condition 1 still holds under Condition 3. Therefore, $r_0 < 0$, $r_1 < 0$, $r_{n_an_bn_c} > 0$ and $r_3 \sim 0$ stand under Condition 3.

Then, the lower bound of V_{111} can be given by

$$V_{111} > \frac{\underline{Q^Z_{vvv}}\cdot\underline{P^{uuu}_{222}} - \overline{Q^Z_{uuu}}\cdot\overline{P^{vvv}_{222}} + (\underline{P^{uuu}_{000}}\,\overline{P^{vvv}_{222}} - \overline{P^{vvv}_{000}}\,\underline{P^{uuu}_{222}})\overline{Q^Z_{000}}}{\overline{P^{vvv}_{111}}\,\underline{P^{uuu}_{222}} - \underline{P^{uuu}_{111}}\,\overline{P^{vvv}_{222}}},$$

and Q^Z_{111} is given by

$$\underline{Q^Z_{111}} = \underline{P^{uuu}_{111}}\frac{\underline{Q^Z_{vvv}}\cdot\underline{P^{uuu}_{222}} - \overline{Q^Z_{uuu}}\cdot\overline{P^{vvv}_{222}} + (\underline{P^{uuu}_{000}}\,\overline{P^{vvv}_{222}} - \overline{P^{vvv}_{000}}\,\underline{P^{uuu}_{222}})\overline{Q^Z_{000}}}{\overline{P^{vvv}_{111}}\,\underline{P^{uuu}_{222}} - \underline{P^{uuu}_{111}}\,\overline{P^{vvv}_{222}}}. \tag{A11}$$

Appendix B: Derivation of a upper bound of e^X_{111}

The quantum bit error rates in X basis can be given by

$$E^X_{\gamma_a\gamma_b\gamma_c}Q^X_{\gamma_a\gamma_b\gamma_c} = \sum_{m_a,m_b,m_c}\sum_{n_a,n_b,n_c} P_{in}(m_am_bm_c)P^{\gamma_a}_{n_a}(m_a) \times P^{\gamma_b}_{n_b}(m_b)P^{\gamma_c}_{n_c}(m_c)Y_{m_{a,b,c}n_{a,b,c}}e_{m_{a,b,c}n_{a,b,c}}.$$

Combining the error rate of untagged pulses $E^X_{\gamma_a\gamma_b\gamma_c}Q^X_{\gamma_a\gamma_b\gamma_c}$ for different intensity settings, we have

$$\begin{aligned} e^X_{111} \le \frac{1}{P^{vvv}_{111}V_{111}}(&E^X_{vvv}Q^X_{vvv} - P^v_0(m_a)E^X_{0vv}Q^X_{0vv} \\ &- P^v_0(m_b)E^X_{v0v}Q^X_{v0v} - P^v_0(m_c)E^X_{vv0}Q^X_{vv0} \\ &+ P^v_0(m_a)P^v_0(m_b)E^X_{00v}Q^X_{00v} \\ &+ P^v_0(m_b)P^v_0(m_c)E^X_{v00}Q^X_{v00} \\ &+ P^v_0(m_a)P^v_0(m_c)E^X_{0v0}Q^X_{0v0} \\ &- P^v_0(m_a)P^v_0(m_b)P^v_0(m_c)E^X_{000}Q^X_{000}). \end{aligned}$$

Then, the upper bound of e^X_{111} is given by

$$\begin{aligned} e^X_{111} \le \frac{1}{\underline{P^{vvv}_{111}}\cdot\underline{V_{111}}}(&\overline{E^X_{vvv}Q^X_{vvv}} - \underline{P^{v_a}_0}\cdot\underline{E^X_{0vv}Q^X_{0vv}} - \underline{P^{v_a}_0}\cdot\underline{E^X_{v0v}Q^X_{v0v}} \\ &- \underline{P^{v_c}_0}\cdot\underline{E^X_{vv0}Q^X_{vv0}} + \overline{P^{v_a}_0}\cdot\overline{P^{v_b}_0}\cdot\overline{E^X_{00v}Q^X_{00v}} \\ &+ \overline{P^{v_b}_0}\cdot\overline{P^{v_c}_0}\cdot\overline{E^X_{v00}Q^X_{v00}} + \overline{P^{v_a}_0}\cdot\overline{P^{v_c}_0}\cdot\overline{E^X_{0v0}Q^X_{0v0}} \\ &- \underline{P^{v_a}_0}\cdot\underline{P^{v_b}_0}\cdot\underline{P^{v_c}_0}\cdot\underline{E^X_{000}Q^X_{000}}). \end{aligned} \tag{B1}$$

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp. 175–179
[2] Lo H K and Chau H F 1999 *Science* **283** 2050
[3] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[4] Mayers D 2001 *J. ACM* **48** 351
[5] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[6] Masanes L, Pironio S and Acín A 2011 *Nat. Commun.* **2** 238
[7] Pironio S, Masanes Ll, Leverrier A and Acín A 2013 *Phys. Rev. X* **3** 031007
[8] Pawłowski M and Brunner N 2011 *Phys. Rev. A* **84** 010302
[9] Wang Y, Bao W S, Li H W, Zhou C and Li Y 2014 *Chin. Phys. B* **23** 080303
[10] Qi B, Fung C H F, Lo H K and Ma X 2007 *Quantum Inf. Comput.* **7** 73
[11] Zhao Y, Fung C H F, Qi B, Chen C and Lo H K 2008 *Phys. Rev. A* **78** 042333
[12] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photonics* **4** 686
[13] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C and Makarov V 2011 *Nat. Commun.* **2** 349
[14] Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, Makarov V and Leuchs G 2011 *Phys. Rev. Lett.* **107** 110501
[15] Jiang M S, Sun S H, Tang G Z, Ma X C, Li C Y and Liang L M 2013 *Phys. Rev. A* **88** 062335
[16] Tanner M G, Makarov V and Hadfield R H 2014 *Opt. Express* **22** 6734
[17] Bugge A N, Sauge S, Ghazali A M M, Skaar J, Lydersen L and Makarov V 2014 *Phys. Rev. Lett.* **112** 070503
[18] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[19] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[20] Tamaki K, Lo H K, Fung C H F and Qi B 2012 *Phys. Rev. A* **85** 042307
[21] Ma X and Razavi M 2012 *Phy. Rev. A* **86** 062319
[22] Wang X B 2013 *Phys. Rev. A* **87** 012320
[23] Xu F, Curty M, Qi B and Lo H K 2013 *New J. Phys.* **15** 113007
[24] Zhou C, Bao W S, Chen W, Li H W, Yin Z Q, Wang Y and Han Z F 2013 *Phys. Rev. A* **88** 052333
[25] Wang Q and Wang X B 2013 *Phys. Rev. A* **88** 052332
[26] Curty M, Xu F, Cui W, Lim C C W, Tamaki K and Lo H K 2014 *Nat. Commun.* **5** 3732
[27] Yin Z Q, Fung C H F, Ma X, Zhang C M, Li H W, Chen W, Wang S, Guo G C and Han Z F 2014 *Phys. Rev. A* **90** 052319
[28] Zhou C, Bao W S, Zhang H L, Li H W, Wang Y, Li Y and Wang X 2015 *Phys. Rev. A* **91** 022313
[29] Xu F 2015 *Phys. Rev. A* **92** 012333
[30] Dong C, Sun Y and Zhao S H 2015 *Acta Phys. Sin.* **64** 140304 (in Chinese)
[31] Wang L, Zhao S M, Gong L Y and Cheng W W 2015 *Chin. Phys. B* **24** 120307
[32] Rubenok A, Slater J A, Chan P, Lucio-Martinez I and Tittel W 2013 *Phys. Rev. Lett.* **111** 130501

[33] Liu Y, Chen T Y, Wang L J, Liang H, Shentu G L, Wang J, Cui K, Yin H L, Liu N L, Li L, Ma X, Pelc J S, Fejer M M, Peng C Z, Zhang Q and Pan J W 2013 *Phys. Rev. Lett.* **111** 130502
[34] Tang Z, Liao Z, Xu F, Qi B, Qian L and Lo H K 2014 *Phys. Rev. Lett.* **112** 190503
[35] Tang Y L, Yin H L, Chen S J, Liu Y, Zhang W J, Jiang X, Zhang L, Wang J, You L X, Guan J Y, Yang D X, Wang Z, Liang H, Zhang Z, Zhou N, Ma X, Chen T Y, Zhang Q and Pan J W 2014 *Phys. Rev. Lett.* **113** 190501
[36] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen C S and Andersen U L 2015 *Nat. Photonics* **9** 397
[37] Tang Y L, Yin H L, Zhao Q, Liu H, Sun X X, Huang M Q, Zhang W J, Chen S J, Zhang L, You L X, Wang Z, Liu Y, Lu C Y, Jiang X, Ma X, Zhang Q, Chen T Y and Pan J W 2016 *Phys. Rev. X* **6** 011024
[38] Comandar L C, Lucamarini M, Fröhlich B, Dynes J F, Sharpe A W, Tam S W B, Yuan Z L, Penty R V and Shields A J 2016 *Nat. Photonics* **10** 312
[39] Wang C, Song X T, Yin Z Q, Wang S, Chen W, Zhang C M, Guo G C and Han Z F 2015 *Phys. Rev. Lett.* **115** 160502
[40] Yin H L, Chen T Y, Yu Z W, Liu H, You L X, Zhou Y H, Chen S J, Mao Y, Huang M Q, Zhang W J, Chen H, Li M J, Nolan D, Zhou F, Jiang X, Wang Z, Zhang Q, Wang X B and Pan J W 2016 *Phys. Rev. Lett.* **117** 190501
[41] Bose S, Vedral V and Knight P L 1998 *Phys. Rev. A* **57** 822
[42] Chen K and Lo H K 2007 *Quantum Inf. Comput.* **7** 689
[43] Fu Y, Yin H L, Chen T Y and Chen Z B 2015 *Phys. Rev. Lett.* **114** 090501
[44] Zhu C, Xu F and Pei C 2015 *Sci. Rep.* **5** 17449
[45] Chen R K, Bao W S, Wang Y, Bao H Z, Zhou C and Li H W 2016 *Opt. Express* **24** 6594
[46] Zhao Y, Qi B and Lo H K 2008 *Phys. Rev. A* **77** 052327
[47] Zhao Y, Qi B, Lo H K and Qian L 2010 *New J. Phys.* **12** 023024
[48] Sajeed S, Radchenko I, Kaiser S, Bourgoin J P, Pappa A, Monat L, Legré M and Makarov V 2015 *Phys. Rev. A* **91** 032326