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

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics
Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
23 January 2022

REVISED
16 May 2022

ACCEPTED FOR PUBLICATION
25 May 2022

PUBLISHED
14 June 2022

Original content from this work may be used under the terms of the Creative Commons Attribution 4.0 licence.

Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

PAPER

Sending-or-not-sending twin field quantum key distribution with imperfect vacuum sources

Xiao-Long Hu[1], Cong Jiang[2], Zong-Wen Yu[3] and Xiang-Bin Wang[2,4,5,6,*]

[1] School of Physics, State Key Laboratory of Optoelectronic Materials and Technologies, Sun Yat-sen University, Guangzhou 510275, People's Republic of China
[2] Jinan Institute of Quantum Technology, SAICT, Jinan 250101, People's Republic of China
[3] Data Communication Science and Technology Research Institute, Beijing 100191, People's Republic of China
[4] State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, People's Republic of China
[5] Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China
[6] Shenzhen Institute for Quantum Science and Engineering, and Physics Department, Southern University of Science and Technology, Shenzhen 518055, People's Republic of China
[*] Author to whom any correspondence should be addressed.

E-mail: xbwang@mail.tsinghua.edu.cn

Keywords: quantum key distribution, sending-or-not-sending protocol, decoy state method, imperfect vacuum source

Abstract

The sending-or-not-sending (SNS) protocol of the twin-field (TF) quantum key distribution (QKD) can tolerant large misalignment error and its key rate can exceed the linear bound of repeaterless QKD. The original SNS protocol and all variants of TF-QKD require perfect vacuum sources, but in the real world experiments there is no practical perfect vacuum source. Instead, experimenters use extremely weak sources to substitute vacuum sources, which may break the security of the protocol. Here we propose an SNS protocol with imperfect vacuum sources and give the non-asymptotic decoy-state analysis of this protocol. Our numerical simulation shows that when the imperfect vacuum sources are close to perfect vacuum sources, our protocol can obtain similar key rate as that with perfect vacuum sources. This is the first result that closes the potential security loophole due to imperfect vacuum of TF-QKD.

1. Introduction

Quantum key distribution (QKD) provides a method for unconditionally secure communication [1–4] between two parties, Alice and Bob. Combined with the decoy-state method [5–7] and measurement-device-independent (MDI) QKD protocol [8, 9], QKD can overcome the security loophole from the nonideal single-photon sources and imperfect detection devices and is demonstrated in several experiments [10–16]. So far, the maximum experimental distance of MDIQKD has reached to 404 km [17] using the four-intensity protocol [18, 19] with parameter optimization [18–21]. With the decoy-state method, the BB84-like QKD has reached a distance of record of 421 km [22]. But the key rate of BB84, MDIQKD protocol, or any modified version of these protocols cannot exceed the linear bounds of repeaterless QKD, the PLOB (Pirandola, Laurenza, Ottaviani, and Banchi) bound [23].

Recently, a new protocol named twin-field (TF) quantum key distribution (TFQKD) was proposed [24] whose key rate dependence on the channel transmittance η is $R \sim O(\sqrt{\eta})$. Since then, the key rate advantage of TFQKD has been extensively demonstrated [25–35]. The efficient protocol for TFQKD, named the sending-or-not-sending (SNS) protocol [36], has the advantage of unconditionally security under coherent attacks and it can tolerant large misalignment error, and the SNS protocol has been widely studied in theories [37–44] and experimentally [25, 26, 29–32, 35]. Notably, the SNS protocol has been demonstrated in the 511 km field test [31], the farthest field experiment to date, linking two metropolitans Jinan and QingDao, and long distance laboratory experiment with vibration detection [35].

© 2022 The Author(s). Published by IOP Publishing Ltd on behalf of the Institute of Physics and Deutsche Physikalische Gesellschaft

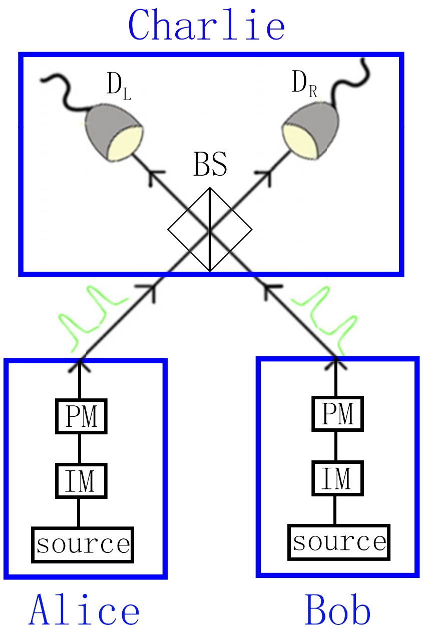

Figure 1. A schematic of the setup for the SNS protocol. IM: intensity modulator; PM: phase modulator; BS: beam-splitter; D_L & D_R: single-photon detector in the measurement station of Charlie.

In the real world experiments, there is no perfect vacuum source [21, 45, 46]. In the existing TF-QKD experiments, the vacuum sources required in the theoretical protocols are replaced by extremely weak sources, which are attenuated from normal lasers and the extinction ratio is imperfect, e.g., in the magnitude order of 50 dB. If these imperfect vacuum sources were used and the final key was still distilled through the original protocol, security loopholes might occur. To avoid the potential security loopholes, we propose an SNS protocol which is secure with imperfect vacuum sources. In this protocol, when Alice (Bob) decides not to send, she (he) actually sends a phase-randomized coherent state with an extremely small intensity. In the view of photon-number space, when sending this coherent state, she (he) sends no photon, i.e. a vacuum state, with a probability close to 1 and sends one or more photons with a very small probability. We will show that even with such imperfect vacuum sources, our protocol is secure with good performance, taken the finite-size effects [38, 41, 47–49] with imperfect devices [45, 46, 50, 51] into consideration. Then we will give the formulas of parameter estimation and the secure key rate in this protocol.

This paper is arranged as follows. In section 2, we present the procedures of our SNS protocol with imperfect vacuum sources. In section 3, we analyze the security of our protocol and give the formulas of the secure key rate according to the decoy-state method. We show the results of numerical simulation of this SNS protocol with imperfect vacuum sources compared with the original four-intensity SNS protocol in section 4. The article ends with some concluding remarks in section 5.

2. SNS protocol with imperfect vacuum sources

The schematic of our protocol is shown in figure 1. We shall also add the actively odd parity pairing (AOPP) in the data post-processing [40–42]. In the decoy-state analysis part, we can apply either three-intensity method or four-intensity method. Here, we take the four-intensity method as an example to introduce the detailed procedures of this protocol as follows.

In each time window, Alice (Bob) randomly decides to prepare and send a phase-randomized weak coherent state (WCS) of intensity μ_z with probability p_z, a extremely WCS of intensity μ_v with probability p_v, a WCS of intensity μ_y with probability p_y and a WCS of intensity μ_x with probability p_x. Surely, $p_z + p_v + p_x + p_y = 1$, and a coherent state of intensity μ with phase θ is $\left|\sqrt{\mu}\,\mathrm{e}^{\mathrm{i}\theta}\right\rangle$. The value of μ_v is very small. Here, the intensities are required to satisfy:

$$\mu_y > \mu_x > \mu_v \geqslant 0. \tag{1}$$

We first consider the case that Alice and Bob are able to control the intensity μ_v precisely. The special case that the intensity μ_v is fixed but unknown will be discussed later.

Then Alice and Bob send their pulses to Charlie; Charlie is assumed to perform interferometric measurements on the received pulses and announce the measuring results to Alice and Bob. If only one of the two detectors clicks, Charlie would announce that this pulse pair causes a click and whether the left detector or the right one clicks. Alice and Bob take it as a one-detector heralded event.

For ease of presentation, we define a time window to be an *lr* window if Alice sends out a coherent state of intensity μ_l and Bob sends out a coherent state of intensity μ_r. In particular, we define all those time windows of *zv*, *vz*, *vv*, and *zz* as *Z* windows and all those time windows of *xx* as *X* windows.

After Alice and Bob repeat the above process many times, Alice (Bob) announces those time windows when she (he) has decided to send a WCS of intensity μ_x and those when she (he) has decided a WCS of intensity μ_y. They use *Z* windows for bit value encoding, in particular, in a *Z* window when Alice (Bob) decides to send a WCS of intensity μ_z, i.e., decides sending, she (he) puts down a bit value 1 (0); in a *Z* window when Alice (Bob) decides to send a WCS of intensity μ_v, i.e., decides not-sending, she (he) puts down a bit value 0 (1). Correspondingly, in *Z* windows, the sending probability of Alice or Bob is

$$\epsilon = \frac{p_z}{p_z + p_v}. \tag{2}$$

A *Z* window when one party decides sending and another party decides not-sending is named as a $\tilde{Z}$ window. In *Z* windows, only those one-detector-heralded events are regarded as effective events that contribute for final key distillation, and the events when Charlie announces two clicks or no click would be discarded. We denote the total number of one-detector-heralded events in *lr* windows as n_{lr}. Here are some more definitions: a *Z* window or $\tilde{Z}$ window producing an effective event is named as an effective *Z* window or an effective $\tilde{Z}$ window. Since the phases in *Z* windows are never announced, the pulses sent in *Z* windows can be regarded as the mixture of different Fock states. For those discarded windows without correct heralding at Charlie's station, they announce which intensity they choose at each window. For those *X* windows, they announce the phases of the WCS they sent, θ_A and θ_B. Among *X* windows, the window in which the phases satisfy

$$1 - |\cos(\theta_\mathrm{A} - \theta_\mathrm{B})| \leqslant \lambda \tag{3}$$

is defined as an X_1 window. Here λ is a positive number close to 0 and its value is determined by Alice and Bob according to the result of channel test and calibration in the experiment to obtain a satisfactory key rate. The data of X_1 windows are used to estimate the phase-flip error rate of untagged bits. The data of other windows are used to perform the decoy-state analysis.

In our protocol, the untagged event is defined by: (1) it is an effective event in a *Z* window; (2) one of Alice and Bob chooses the intensity μ_z and he/she actually sends a one-photon pulse, and the other of them chooses the intensity μ_v and he/she actually sends a vacuum pulse. The bits from these untagged events are defined as untagged bits.

Finally, Alice and Bob perform the postprocessing and obtain the final key with length [38]

$$N_\mathrm{f} = n_\mathrm{u}^\mathrm{L}[1 - H(e_\mathrm{u}^\mathrm{ph,U})] - f n_Z H(E_Z) - \log_2 \frac{2}{\varepsilon_\mathrm{cor}} - 2\log_2 \frac{1}{\sqrt{2}\varepsilon_\mathrm{PA}\hat{\varepsilon}}. \tag{4}$$

With the key length formula equation (4), the security coefficient of the whole protocol [47, 48] is

$$\varepsilon_\mathrm{tol} = \varepsilon_\mathrm{cor} + 2\hat{\varepsilon} + \varepsilon_\mathrm{PA} + 4\sqrt{\varepsilon_\mathrm{e} + \varepsilon_{n_\mathrm{u}}}. \tag{5}$$

Here, n_u^L is the lower bound of the number of untagged bits; $e_\mathrm{u}^\mathrm{ph,U}$ is the upper bound of the phase-flip error rate of untagged bits; *f* is the error correction inefficiency; n_Z is the number of effective events in *Z* windows; E_Z is the bit-flip error rate of effective events in *Z* windows; $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the Shannon entropy; ε_cor is the failure probability of error correction; ε_PA is the failure probability of privacy amplification; $\hat{\varepsilon}$ is the coefficient while using the chain rules of max- and min-entropy [38]; ε_e is the failure probability of the estimation of phase-flip error rate; and $\varepsilon_{n_\mathrm{u}}$ is the failure probability of the estimation of the number of untagged bits.

To further improve the secure key rate and distance, we apply AOPP [40–42] here: Alice does AOPP for her bits from effective *Z* windows (she makes odd pairs of her bits from effective *Z* windows randomly) and then takes parity check with Bob for each pair. Those pairs with odd parity values at Bob's side will survive. They take one bit randomly from every survived pair and then distill the final key with the following key length

$$N_{\mathrm{f}}' = n_{\mathrm{u}}'[1 - H(e_{\mathrm{u}}'^{\mathrm{ph}})] - f n_Z' H(E_Z') - 2\left(\log_2 \frac{2}{\varepsilon_{\mathrm{cor}}} - 2\log_2 \frac{1}{\sqrt{2}\varepsilon_{\mathrm{PA}}\hat{\varepsilon}}\right), \tag{6}$$

where n_{u}' and $e_{\mathrm{u}}'^{ph}$ are the number and the phase-flip error rate of survived untagged bits after AOPP, respectively, and n_Z' and E_Z' are the number and the bit-flip error rate of all survived bits after AOPP, respectively. Note that the finite-key analysis in references [38, 41, 42] still works in this protocol.

The quantum communication part of our protocol above is identical to that of the original SNS protocol, except that the exact vacuum is replaced by the supposed vacuum, the coherent state with intensity μ_v. However, without using any vacuum in the SNS protocol, it is unknown so far how to efficiently verify the lower bound of untagged bits and upper bound of phase-flip error rate of single-photon bits, i.e., the lower bound of n_{u}' and the upper bound of $e_{\mathrm{u}}'^{\mathrm{ph}}$ in equation (6) above. Now we show this.

3. Decoy-state analysis

Since the phases of the WCS in Z windows are never announced, these states can be regarded as the mixture of different Fock states, i.e. the density matrix of the WCS with intensity μ_l can be written as

$$\rho(\mu_l) = \sum_{m=0}^{\infty} l_m \left|m\right\rangle \left\langle m\right|, \tag{7}$$

where $l_m = \mathrm{e}^{-\mu_l}\frac{\mu_l^m}{m!}$. Thus, in Z windows, the TF state sent by Alice and Bob is

$$\rho_{lr} = \sum_{m,n=0}^{\infty} l_m r_n \left|mn\right\rangle \left\langle mn\right|, \quad lr = vv, vz, zv, zz. \tag{8}$$

For simplicity, we assume that Alice's and Bob's intensities of sources v are the same in this section. In general, they can be different, i.e., Alice and Bob have their own intensities $\mu_{v\mathrm{A}}$ and $\mu_{v\mathrm{B}}$. But this will not affect the security and the decoy-state analysis here still works except that the formulas are more complicated. We will give the formulas with asymmetric μ_v in the appendix.

Correspondingly, the density matrix of all pulses in Z windows is

$$\rho_Z = (1-\epsilon)^2 \rho_{vv} + \epsilon^2 \rho_{zz} + \epsilon(1-\epsilon)(\rho_{vz} + \rho_{zv}). \tag{9}$$

With equation (8), we have

$$\frac{\rho_{vz} + \rho_{zv}}{2} = v_0 z_1 \rho_{\mathrm{u}} + (1 - v_0 z_1)\tilde{\rho}_{\mathrm{u}}, \tag{10}$$

where ρ_{u} is the density matrix of the TF states of untagged bits

$$\rho_{\mathrm{u}} = \frac{\left|10\right\rangle\left\langle 10\right| + \left|01\right\rangle\left\langle 01\right|}{2} \tag{11}$$

and it is easy to prove that $\tilde{\rho}_{\mathrm{u}}$ is also a density matrix. So ρ_Z is a classical mixture of the state ρ_{u} and some other states. According to the tagged model [52, 53], we can regard bits from the state ρ_{u} in Z windows as untagged bits and those from other states in Z windows as tagged bits. As long as we can estimate the lower bound of the number of untagged bits and the upper bound of the phase-flip error rate of untagged bits with the decoy-state method, we can use the formula in equation (4) to calculate the secure key length.

For convenience, we introduce some virtual sources that emit pulses of a certain photon number, and the corresponding states are $\rho_m = \left|m\right\rangle\left\langle m\right|$. The subscript lr introduced above can be generalized to the combination of these virtual sources. For example, ρ_{z1} denotes the TF state when Alice sends pulses of WCS with intensity μ_z and Bob sends pulses containing one photon; ρ_{11} denotes the TF state when both Alice and Bob send pulses containing one photon.

We define the counting rate of a TF state from real sources as $S_{lr} = n_{lr}/N_{lr}$, where N_{lr} is the total number of pulse pairs lr sent by Alice and Bob and n_{lr} is the number of one-detector heralded events caused by pulse pairs lr. Similarly, we define the counting rate of a TF state from virtual sources as $s_{lr} = n_{lr}/N_{lr}$, where at least one of l and r is a virtual source. Note that values of S_{lr} can be observed in the experiment, but s_{lr} cannot. The expected values of S_{lr} (s_{lr}) are defined as $\langle S_{lr}\rangle$ ($\langle s_{lr}\rangle$), and the relation among them is given by Chernoff bound [48, 54] shown in the appendix. In the following, we will show how to estimate the lower bound of $\langle s_{01}\rangle$ and $\langle s_{10}\rangle$.

According to the decoy-state method [5–7], we have

$$\begin{aligned}\langle s_{0v}\rangle &= v_0\langle s_{00}\rangle + v_1\langle s_{01}\rangle + v_2\langle s_{02}\rangle + \sum_{n=3}^{\infty} v_n\langle s_{0n}\rangle,\\ \langle s_{0x}\rangle &= x_0\langle s_{00}\rangle + x_1\langle s_{01}\rangle + x_2\langle s_{02}\rangle + \sum_{n=3}^{\infty} x_n\langle s_{0n}\rangle,\\ \langle s_{0y}\rangle &= y_0\langle s_{00}\rangle + y_1\langle s_{01}\rangle + y_2\langle s_{02}\rangle + \sum_{n=3}^{\infty} y_n\langle s_{0n}\rangle.\end{aligned} \tag{12}$$

By eliminating the terms $\langle s_{00}\rangle$ and $\langle s_{02}\rangle$, we can get

$$\langle s_{01}\rangle = \frac{v_0[(y_2v_0 - y_0v_2)\langle s_{0x}\rangle - (x_2v_0 - x_0v_2)\langle s_{0y}\rangle - (y_2x_0 - y_0x_2)\langle s_{0v}\rangle]}{(y_2v_0 - y_0v_2)(x_1v_0 - x_0v_1) - (x_2v_0 - x_0v_2)(y_1v_0 - y_0v_1)} + \xi_1, \tag{13}$$

and the term ξ_1 can be proved to be non-negative (detailed derivation is given in the appendix). Thus, we can obtain the lower bound of $\langle s_{01}\rangle$

$$\langle s_{01}\rangle \geqslant \langle s_{01}\rangle^{\mathrm{L}} = \frac{v_0[(y_2v_0 - y_0v_2)\langle s_{0x}\rangle^{\mathrm{L}} - (x_2v_0 - x_0v_2)\langle s_{0y}\rangle^{\mathrm{U}} - (y_2x_0 - y_0x_2)\langle s_{0v}\rangle^{\mathrm{U}}]}{(y_2v_0 - y_0v_2)(x_1v_0 - x_0v_1) - (x_2v_0 - x_0v_2)(y_1v_0 - y_0v_1)}, \tag{14}$$

assuming that we know the bounds of $\langle s_{0x}\rangle$, $\langle s_{0y}\rangle$, and $\langle s_{0v}\rangle$. Here, the superscript L stands for the lower bound of this quantity and U stands for the upper bound of this quantity. Similarly, we can obtain the lower bound of $\langle s_{10}\rangle$:

$$\langle s_{10}\rangle \geqslant \langle s_{10}\rangle^{\mathrm{L}} = \frac{v_0[(y_2v_0 - y_0v_2)\langle s_{x0}\rangle^{\mathrm{L}} - (x_2v_0 - x_0v_2)\langle s_{y0}\rangle^{\mathrm{U}} - (y_2x_0 - y_0x_2)\langle s_{v0}\rangle^{\mathrm{U}}]}{(y_2v_0 - y_0v_2)(x_1v_0 - x_0v_1) - (x_2v_0 - x_0v_2)(y_1v_0 - y_0v_1)}, \tag{15}$$

assuming that we know the bounds of $\langle s_{x0}\rangle$, $\langle s_{y0}\rangle$, and $\langle s_{v0}\rangle$.

With the expansion of $\langle S_{vv}\rangle$

$$\begin{aligned}\langle S_{vv}\rangle &= v_0\langle s_{0v}\rangle + v_1\langle s_{1v}\rangle + \sum_{n=2}^{\infty} v_n\langle s_{nv}\rangle\\ &= v_0\langle s_{0v}\rangle + v_1\left(v_0\langle s_{10}\rangle + \sum_{m=1}^{\infty} v_m\langle s_{1m}\rangle\right) + \sum_{n=2}^{\infty} v_n\langle s_{nv}\rangle,\end{aligned} \tag{16}$$

we can easily get

$$\langle s_{0v}\rangle \leqslant \frac{1}{v_0}\langle S_{vv}\rangle - v_1\langle s_{10}\rangle \leqslant \frac{1}{v_0}\langle S_{vv}\rangle - v_1\langle s_{10}\rangle^{\mathrm{L}}. \tag{17}$$

Thus,

$$\langle s_{0v}\rangle^{\mathrm{U}} = \frac{1}{v_0}\langle S_{vv}\rangle - v_1\langle s_{10}\rangle^{\mathrm{L}}. \tag{18}$$

Similarly, we have

$$\begin{aligned}\langle s_{v0}\rangle^{\mathrm{U}} &= \frac{1}{v_0}\langle S_{vv}\rangle - v_1\langle s_{01}\rangle^{\mathrm{L}},\\ \langle s_{0y}\rangle^{\mathrm{U}} &= \frac{1}{v_0}\langle S_{vy}\rangle - \frac{v_1y_0}{v_0}\langle s_{10}\rangle^{\mathrm{L}},\\ \langle s_{y0}\rangle^{\mathrm{U}} &= \frac{1}{v_0}\langle S_{yv}\rangle - \frac{v_1y_0}{v_0}\langle s_{01}\rangle^{\mathrm{L}}.\end{aligned} \tag{19}$$

With the expansion of $\langle S_{vx}\rangle$ and $\langle S_{xx}\rangle$

$$\begin{aligned}\langle S_{vx}\rangle &= v_0\langle s_{0x}\rangle + v_1\langle s_{1x}\rangle + \sum_{n=2}^{\infty} v_n\langle s_{nx}\rangle,\\ \langle S_{xx}\rangle &= x_0\langle s_{0x}\rangle + x_1\langle s_{1x}\rangle + \sum_{n=2}^{\infty} x_n\langle s_{nx}\rangle,\end{aligned} \tag{20}$$

by eliminating $\langle s_{1x}\rangle$, we can get

$$\langle s_{0x}\rangle^{\mathrm{L}} = \frac{x_1\langle S_{vx}\rangle - v_1\langle S_{xx}\rangle}{x_1v_0 - x_0v_1}. \tag{21}$$

Similarly, we have

$$\langle s_{x0}\rangle^{\mathrm{L}} = \frac{x_1\langle S_{xv}\rangle - v_1\langle S_{xx}\rangle}{x_1 v_0 - x_0 v_1}. \tag{22}$$

Combining equations (14), (15), (18), (19), (21) and (22), and substituting $l_m = \mathrm{e}^{-\mu_l}\frac{\mu_l^m}{m!}, l = v, x, y$, we can obtain $\langle s_{01}\rangle^{\mathrm{L}}$ and $\langle s_{10}\rangle^{\mathrm{L}}$:

$$\langle s_{01}\rangle^{\mathrm{L}} = \frac{g_3(g_1\langle S_{vx}\rangle + g_2\langle S_{xv}\rangle) - [g_4(g_1+g_2)\langle S_{xx}\rangle + g_5(g_1\langle S_{vy}\rangle + g_2\langle S_{yv}\rangle) + g_6(g_1+g_2)\langle S_{vv}\rangle]}{g_1^2 - g_2^2}, \tag{23}$$

$$\langle s_{10}\rangle^{\mathrm{L}} = \frac{g_3(g_1\langle S_{xv}\rangle + g_2\langle S_{vx}\rangle) - [g_4(g_1+g_2)\langle S_{xx}\rangle + g_5(g_1\langle S_{yv}\rangle + g_2\langle S_{vy}\rangle) + g_6(g_1+g_2)\langle S_{vv}\rangle]}{g_1^2 - g_2^2}, \tag{24}$$

if $g_1^2 - g_2^2 > 0$, where

$$\begin{aligned}
g_1 &= (\mu_y - \mu_v)(\mu_x - \mu_v)(\mu_y - \mu_x),\\
g_2 &= \mu_v(\mu_y^2 - \mu_v^2),\\
g_3 &= \mathrm{e}^{\mu_x+\mu_v}\frac{\mu_x}{\mu_x - \mu_v}(\mu_y^2 - \mu_v^2),\\
g_4 &= e^{2\mu_x}\frac{\mu_v}{\mu_x - \mu_v}(\mu_y^2 - \mu_v^2),\\
g_5 &= \mathrm{e}^{\mu_y+\mu_v}(\mu_x^2 - \mu_v^2),\\
g_6 &= e^{2\mu_v}(\mu_y^2 - \mu_x^2).
\end{aligned}$$

Thus, the counting rate of the untagged pulse pairs in state ρ_{u} is:

$$\langle s_{\mathrm{u}}\rangle^{\mathrm{L}} = \frac{\langle s_{01}\rangle^{\mathrm{L}} + \langle s_{10}\rangle^{\mathrm{L}}}{2} = \frac{S_+ - S_-}{g_1^2 - g_2^2}, \tag{25}$$

where

$$S_+ = g_3\frac{\langle S_{vx}\rangle + \langle S_{xv}\rangle}{2} \tag{26}$$

and

$$S_- = g_4\langle S_{xx}\rangle + g_5\frac{\langle S_{vy}\rangle + \langle S_{yv}\rangle}{2} + g_6\langle S_{vv}\rangle. \tag{27}$$

If $g_1^2 - g_2^2 \leqslant 0$, $\langle s_{01}\rangle^{\mathrm{L}} = \langle s_{10}\rangle^{\mathrm{L}} = \langle s_{\mathrm{u}}\rangle^{\mathrm{L}} = 0$ and thus no final key will be obtained. In the calculation of equations (23), (24), (26) and (27), we can use the joint constrains of statistical fluctuation [20] to reduce the effects of statistical fluctuation.

With equations (9) and (10), we can obtain the lower bound of the expected number of the untagged bits:

$$\langle n_{\mathrm{u}}\rangle^{\mathrm{L}} = 2N_Z\epsilon(1-\epsilon)v_0 z_1\langle s_{\mathrm{u}}\rangle^{\mathrm{L}}, \tag{28}$$

where N_Z is the number of Z windows. In equation (25), if we set $\mu_v = 0$, which means that we have perfect vacuum sources, the formula of the counting rate of the untagged pulse pairs is exactly the same as that in the original four-intensity SNS protocol [37].

As proved in reference [37], the density matrix of the TF state in X_1 windows can be written as a mixture of n-photon TF states

$$\rho_{X_1} = \mathrm{e}^{-2\mu_x}\sum_{n=0}^{\infty}\frac{(2\mu_x)^n}{n!}\sigma_n \tag{29}$$

and these n-photon TF states are

$$\sigma_n = \frac{1}{2\phi}\int_{-\phi}^{\phi}\frac{1}{2}\left(\left|\psi_n^+(\delta)\right\rangle\left\langle\psi_n^+(\delta)\right| + \left|\psi_n^-(\delta)\right\rangle\left\langle\psi_n^-(\delta)\right|\right)\mathrm{d}\delta, \tag{30}$$

where $\phi = \arccos(1-\lambda)$,

$$\left|\psi_n^+(\delta)\right\rangle = \frac{1}{\sqrt{2^n}}\sum_{m=0}^{n}\frac{\sqrt{n!}\mathrm{e}^{\mathrm{i}m\delta}}{\sqrt{m!(n-m)!}}\left|m\right\rangle\left|n-m\right\rangle, \tag{31}$$

and

$$\left|\psi_n^-(\delta)\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{m=0}^{n} \frac{(-1)^m \sqrt{n!} e^{im\delta}}{\sqrt{m!(n-m)!}} |m\rangle |n-m\rangle . \tag{32}$$

We can find that $\sigma_0 = \rho_{00}$ and $\sigma_1 = \rho_{\mathrm{u}}$. So the single-photon state in X_1 windows and that in Z windows have the same density matrices. With this relations, the phase-flip error rate $e_{\mathrm{u}}^{\mathrm{ph}}$ can be estimated asymptotically through the single-photon state σ_1 in X_1 windows.

We define the error counting rate of a set C as $T_C = m_C/N_C$, where N_C is the total number of instances in the set C and m_C is the number of *wrong* one-detector heralded events in the set C. We use the lowercase t_C when the sources in the set C are virtual sources. The expected values of T_C and t_C are defined as $\langle T_C\rangle$ and $\langle t_C\rangle$, respectively.

The error counting rate of X_1 windows can be written as

$$\langle T_{X_1}\rangle = e^{-2\mu_x} \left[\langle t_{\sigma_0}\rangle + 2\mu_x \langle t_{\sigma_1}\rangle + \sum_{n=2}^{\infty} \frac{(2\mu_x)^n}{n!} \langle t_{\sigma_n}\rangle \right]. \tag{33}$$

Using the relations $\sigma_0 = \rho_{00}$ and $\sigma_1 = \rho_{\mathrm{u}}$, we can have

$$\langle t_{\mathrm{u}}\rangle \leqslant \langle t_{\mathrm{u}}\rangle^{\mathrm{U}} = \frac{\langle T_{X_1}\rangle - e^{-2\mu_x}\langle t_{00}\rangle^{\mathrm{L}}}{2\mu_x\, e^{-2\mu_x}}. \tag{34}$$

With the expansion of $\langle S_{vv}\rangle$ and $\langle S_{xx}\rangle$

$$\begin{aligned} \langle S_{vv}\rangle &= v_0^2\langle s_{00}\rangle + v_0 v_1(\langle s_{01}\rangle + \langle s_{10}\rangle) + \sum_{\substack{m,n\geqslant 0\\ m+n>1}} v_m v_n \langle s_{mn}\rangle, \\ \langle S_{xx}\rangle &= x_0^2\langle s_{00}\rangle + x_0 x_1(\langle s_{01}\rangle + \langle s_{10}\rangle) + \sum_{\substack{m,n\geqslant 0\\ m+n>1}} x_m x_n \langle s_{mn}\rangle, \end{aligned} \tag{35}$$

by eliminating $(\langle s_{01}\rangle + \langle s_{10}\rangle)$, we can get

$$\langle s_{00}\rangle^{\mathrm{L}} = e^{2\mu_v} \frac{\mu_x}{\mu_x - \mu_v}\langle S_{vv}\rangle - e^{2\mu_x}\frac{\mu_v}{\mu_x - \mu_v}\langle S_{xx}\rangle. \tag{36}$$

Using the fact that the error rate of vacuum pulses is 1/2 asymptotically [55], i.e. $\langle t_{00}\rangle = \langle s_{00}\rangle/2$, we can obtain the upper bound of the phase-flip error rate of untagged bits:

$$\begin{aligned} \langle e_{\mathrm{u}}^{\mathrm{ph}}\rangle^{\mathrm{U}} &= \frac{\langle t_{\mathrm{u}}\rangle^{\mathrm{U}}}{\langle s_{\mathrm{u}}\rangle^{\mathrm{L}}} \\ &= \frac{\langle T_{X_1}\rangle + \frac{\mu_v}{2(\mu_x-\mu_v)}\langle S_{xx}\rangle - e^{2(\mu_v-\mu_x)}\frac{\mu_x}{2(\mu_x-\mu_v)}\langle S_{vv}\rangle}{2\mu_x\, e^{-2\mu_x}\langle s_{\mathrm{u}}\rangle^{\mathrm{L}}}. \end{aligned} \tag{37}$$

After obtaining the bounds of $\langle s_{01}\rangle$, $\langle s_{01}\rangle$, and $\langle e_{\mathrm{u}}^{\mathrm{ph}}\rangle$ in equations (23), (24) and (37), we can use the method proposed in references [41, 42] to calculate the bounds of n_{u}' and $e_{\mathrm{u}}'^{\mathrm{ph}}$ after AOPP, and then substitute them into equation (6) to calculate the final key length. The related formulas are shown in the appendix.

3.1. A special case with an unknown intensity of source v

The intensity μ_v is so low that in a real experiment this intensity may not be controlled precisely. When using the source v, Alice (Bob) may send a WCS state with an unknown intensity $\mu_{v\mathrm{A}}'$ ($\mu_{v\mathrm{B}}'$). But they can evaluate their devices to give a convincing upper bound of this unknown intensity, $\bar{\mu}_v$. That is to say, the actual intensities $\mu_{v\mathrm{A}}'$ and $\mu_{v\mathrm{B}}'$ are in a range $[0, \bar{\mu}_v]$.

Using the revised key rate formulas with asymmetric μ_v in the appendix, given the observed data and other source parameters, we can regard the final key length as a function of Alice's and Bob's intensities $\mu_{v\mathrm{A}}$ and $\mu_{v\mathrm{B}}$, i.e. $N_{\mathrm{f}}'(\mu_{v\mathrm{A}}, \mu_{v\mathrm{B}})$. We scan $N_{\mathrm{f}}'(\mu_{v\mathrm{A}}, \mu_{v\mathrm{B}})$ over the range $\mu_{v\mathrm{A}}, \mu_{v\mathrm{B}} \in [0, \bar{\mu}_v]$, find the minimum value $N_{\mathrm{f,min}}'$ as the worst case. Since $N_{\mathrm{f,min}}' \leqslant N_{\mathrm{f}}'(\mu_{v\mathrm{A}}', \mu_{v\mathrm{B}}')$ and $N_{\mathrm{f}}'(\mu_{v\mathrm{A}}', \mu_{v\mathrm{B}}')$ is a secure key length, we can regard $N_{\mathrm{f,min}}'$ as a secure key length as well. In this way, we can guarantee the security of the final key even if we do not know the exact value of the intensity of source v.

According to our numerical results, the worst case always occurs when one of $\mu_{v\mathrm{A}}$ and $\mu_{v\mathrm{B}}$ is the minimum and the other is the maximum of the range, i.e. $\mu_{v\mathrm{A}} = 0, \mu_{v\mathrm{B}} = \bar{\mu}_v$ or $\mu_{v\mathrm{A}} = \bar{\mu}_v, \mu_{v\mathrm{B}} = 0$. Compared with the numerical results with known intensities $\mu_{v\mathrm{A}} = \mu_{v\mathrm{B}} = \bar{\mu}_v$, this special case introduces about 1% extra loss to the final key rate.

Table 1. Devices' parameters used in numerical simulations. N_t is the total number of pulse pairs; e_d is the misalignment error in X windows; d is the dark count rate per pulse of each detector at Charlie's side; η_d is the detection efficiency of each detector at Charlie's side; f is the error correction inefficiency; ξ is the failure probability in the parameter estimation; α is the channel loss.

N_t	e_d	d	η_d	f	ξ	α
10^{12}	1.5%	10^{-10}	50%	1.1	10^{-10}	0.2 dB km^{-1}

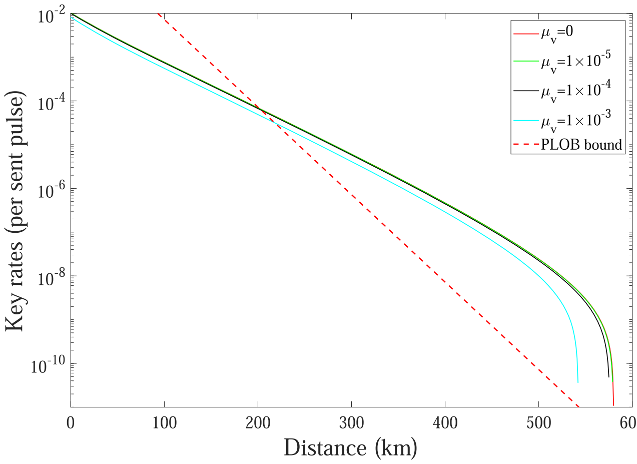

Figure 2. The optimized key rates (per pulse pair) versus transmission distance of our protocol with imperfect vacuum sources with different μ_v.

Security in this special case. (a) As stated in reference [39], the constraint for source parameters is only necessary in the X_1 windows. Therefore, the asymmetric intensities of sources v do not have to satisfy the constraint in reference [39] to guarantee the security. (b) In Z windows, we choose the same amount of pulses in states ρ_{01} and ρ_{10} to constitute the untagged bits (see equation (B16) in the appendix). So the TF state of untagged bits ρ_u remains the same as that in equation (11) and thus the previous security proof still works even if $\mu_{vA} \neq \mu_{vB}$.

4. Numerical simulation

In this part, we show the results of numerical simulation of our AOPP-SNS protocol with imperfect vacuum sources, and compare them with the results of the original AOPP-SNS protocol with perfect vacuum sources [41, 42]. The results will be shown in the form of key rate per pulse, i.e. $R = N_f'/N_t$, where N_f' is the secure key length and N_t is the total number of pulse pairs that Alice and Bob send. The device parameters used in the simulation are listed in table 1. We shall estimate what values would be probably observed in the normal cases by the linear models as previously.

Firstly, we suppose that Alice and Bob know the exact value of the intensity μ_v. We fix the value of μ_v and optimize other source parameters (the intensities and the probabilities of choosing each source) globally to obtain the highest key rate. In figure 2 and table 2, we show the key rates versus transmission distance with different μ_v. When μ_v becomes larger, the key rate will decrease. Compared with the case with perfect vacuum sources ($\mu_v = 0$), as long as μ_v is less than 1×10^{-4}, the decrease of the key rate of our protocol with imperfect vacuum sources is less than 10%. Even if μ_v is as large as 1×10^{-3}, the key rates of our protocol can still exceed the PLOB bound a lot.

Some detailed results of this simulation are shown in table 3. According to the data in table 3, we can find that the decrease of the key rate mainly comes from the increase of the bit-flip error in Z windows caused by the imperfect vacuum sources, which is inevitable when there is no perfect vacuum source in real world experiments. The decoy-state analysis of our protocol gives almost the same n_u' and $e_u'^{ph}$ as the case with perfect vacuum sources. Thanks to the AOPP method [41, 42], the bit-flip error rate can be decreased a lot. Without AOPP, the bit-flip error caused by the imperfect vacuum will decrease the key rate more.

We consider another scenario: in an experiment, Alice and Bob have already used imperfect vacuum sources and have got the corresponding observed data. We compare the results with the decoy-state analysis

Table 2. The optimized key rates (per pulse pair) at some transmission distance with different μ_v.

μ_v	200 km	300 km	400 km	500 km
0	6.99×10^{-5}	6.10×10^{-6}	4.69×10^{-7}	2.44×10^{-8}
1×10^{-5}	6.95×10^{-5}	6.06×10^{-6}	4.66×10^{-7}	2.41×10^{-8}
5×10^{-5}	6.83×10^{-5}	5.95×10^{-6}	4.55×10^{-7}	2.33×10^{-8}
1×10^{-4}	6.70×10^{-5}	5.82×10^{-6}	4.43×10^{-7}	2.24×10^{-8}
5×10^{-4}	5.82×10^{-6}	4.99×10^{-7}	3.67×10^{-7}	1.62×10^{-8}
1×10^{-3}	4.89×10^{-6}	4.11×10^{-7}	2.89×10^{-7}	9.99×10^{-9}

Table 3. Some data at the transmission distance of 400 km with different μ_v. The device parameters used in the simulation are listed in table 1. The source parameters are set as: $\mu_z = 0.501$, $\mu_x = 0.0644$, $\mu_y = 0.337$, $p_x = 0.096$, $p_y = 0.004$, $p_v = 0.649$, and $p_z = 0.251$.

μ_v	n'_{u}	$e_{\mathrm{u}}^{\prime\mathrm{ph}}$	E'_Z	R
0	7.68×10^5	7.61%	1.60×10^{-5}	4.69×10^{-7}
1×10^{-5}	7.68×10^5	7.62%	9.58×10^{-5}	4.66×10^{-7}
5×10^{-5}	7.67×10^5	7.64%	4.15×10^{-4}	4.55×10^{-7}
1×10^{-4}	7.67×10^5	7.66%	8.13×10^{-4}	4.43×10^{-7}
5×10^{-4}	7.63×10^5	7.80%	3.98×10^{-3}	3.66×10^{-7}
1×10^{-3}	7.58×10^5	7.96%	7.91×10^{-3}	2.83×10^{-7}

Table 4. The optimized key rates (per pulse pair) at some transmission distance with different μ_v with the decoy-state analysis of our protocol and that of the original AOPP-SNS protocol in reference [42], respectively. Assume that the observed data were obtained in the QKD process with imperfect vacuum sources.

μ_v		300 km	400 km	500 km
1×10^{-5}	This work	6.06×10^{-6}	4.66×10^{-7}	2.41×10^{-8}
	Reference [42]	6.07×10^{-6}	4.66×10^{-7}	2.42×10^{-8}
1×10^{-4}	This work	5.82×10^{-6}	4.43×10^{-7}	2.24×10^{-8}
	Reference [42]	5.86×10^{-6}	4.47×10^{-7}	2.26×10^{-8}

of the original AOPP-SNS protocol (reference [42]), pretending the non-vacuum source v to be exact vacuum, and the results of our protocol with imperfect vacuum sources (this work), in table 4. From these results, we can see that, as long as μ_v is less than 1×10^{-4}, with given observed data, the decrease of the key rate of our protocol is less than 1%.

In addition, we show the key rates versus the intensity μ_v at a distance of 500 km. Similarly to the simulations above, here we consider two cases:

(a) The expected observed data are simulated with different intensities μ_v and other source parameters have been optimized globally. This case shows how badly μ_v using in experiments affects the key rates. Results are presented in figure 3.

(b) In the simulation of observed data, we use fixed source parameters, including $\mu_v = 1 \times 10^{-4}$. In the calculation of key rate, we assume that μ_v is unknown and calculate the key rate with different upper bounds $\bar{\mu}_v$ using the method in the subsection IIIA. Results are presented in figure 4.

From these results, we can find that in both cases, the key rate decreases when μ_v becomes larger. When μ_v is small enough, the key rate is close to that with a perfect vacuum source ($\mu_v = 0$).

Similar to references [55–58], we can add n_0 bits to the final key length in equation (6), where n_0 is the number of Alice's vacuum-related private bits as shown in the appendix. With this term, we have

$$N''_{\mathrm{f}} = n_0 + N'_{\mathrm{f}}. \tag{38}$$

Surely, we can also use the following more efficient key-length formula

$$\tilde{N}''_{\mathrm{f}} = \min_{\langle S_{vv} \rangle} N''_{\mathrm{f}}(\langle S_{vv} \rangle), \tag{39}$$

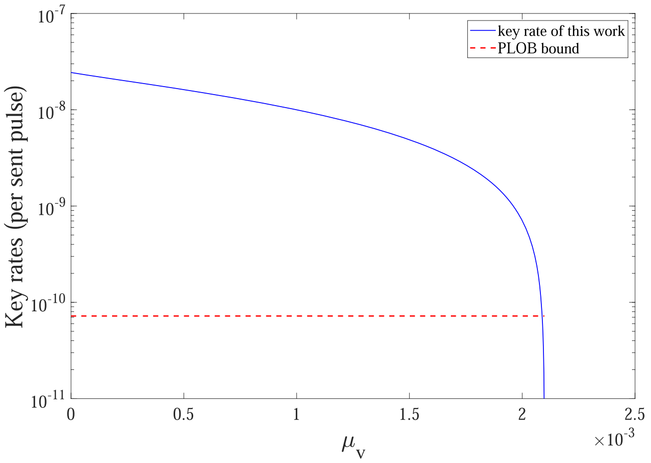

Figure 3. The optimized key rates (per pulse pair) versus the intensity μ_v at a distance of 500 km. The expected observed data are simulated with different intensities μ_v and other source parameters have been optimized globally.

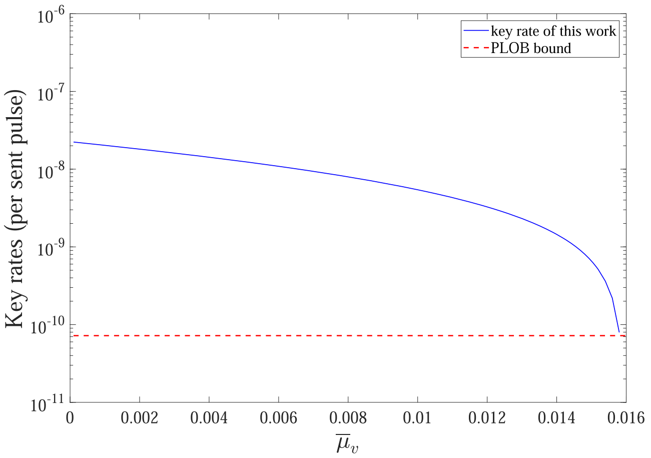

Figure 4. The optimized key rates (per pulse pair) versus the upper bound $\bar{\mu}_v$ at a distance of 500 km. In the simulation of observed data, we use fixed source parameters: $\mu_v = 1 \times 10^{-4}$, $\mu_z = 0.500$, $\mu_x = 0.0794$, $\mu_y = 0.460$, $p_x = 0.171$, $p_y = 0.009$, $p_v = 0.593$, and $p_z = 0.227$. In the calculation of key rate, we assume that μ_v is unknown and calculate the key rate with different upper bound $\bar{\mu}_v$ using the method in the subsection 3.1.

i.e. by scanning $\langle S_{vv}\rangle$ in its possible range for the worst-case result of $N_{\rm f}''$ instead of taking worst-case separately for $s_{\rm u}$ and $e_{\rm u}^{\rm ph}$, can improve the non-asymptotic key rate a little bit. We have not applied equations (38) and (39) in our numerical simulation above.

In summary, even if there is no perfect vacuum sources in practice, the SNS experiments are still secure and give satisfactory key rates.

5. Conclusion

In this paper, we proposed an SNS protocol with imperfect vacuum sources and give the key rate formulas of our protocol. Our protocol can avoid the security loopholes caused by imperfect vacuum sources in real world experiments. According to the numerical simulation, as long as the experiments replace the vacuum source by an extremely weak coherent source and its intensity is less than 1×10^{-4}, the difference of key rates between our protocol with imperfect vacuum sources and that with perfect vacuum sources is less than 10%, and the key rates of our protocol can still exceed the PLOB bound a lot.

The SNS protocol with imperfect vacuum sources with asymmetric channels will be studied in our future research.

Acknowledgments

We acknowledge the financial support in part by National Natural Science Foundation of China Grants Nos. 12147107, 11974204, 12174215, and 12104184; Open Research Fund Program of the State Key Laboratory of Low-Dimensional Quantum Physics Grant No. KF202110.

Data availability statement

The data that support the findings of this study are available upon reasonable request from the authors.

Appendix A. Proof for $\xi_1 \geqslant 0$ in (13)

Remind the relation

$$\mu_y > \mu_x > \mu_v \geqslant 0. \tag{A1}$$

The formula of ξ_1 is

$$\begin{aligned}\xi_1 &= \sum_{n=3}^{\infty} \frac{(y_n v_0 - y_0 v_n)(x_2 v_0 - x_0 v_2) - (x_n v_0 - x_0 v_n)(y_2 v_0 - y_0 v_2)}{(y_2 v_0 - y_0 v_2)(x_1 v_0 - x_0 v_1) - (x_2 v_0 - x_0 v_2)(y_1 v_0 - y_0 v_1)} \langle s_{0n} \rangle \\ &= \sum_{n=3}^{\infty} \frac{1}{n!} \frac{(\mu_y^n - \mu_v^n)(\mu_x^2 - \mu_v^2) - (\mu_x^n - \mu_v^n)(\mu_y^2 - \mu_v^2)}{(\mu_y^2 - \mu_v^2)(\mu_x - \mu_v) - (\mu_x^2 - \mu_v^2)(\mu_y - \mu_v)} \langle s_{0n} \rangle. \end{aligned} \tag{A2}$$

The denominator can be rewritten as

$$(\mu_y^2 - \mu_v^2)(\mu_x - \mu_v) - (\mu_x^2 - \mu_v^2)(\mu_y - \mu_v) = (\mu_y - \mu_v)(\mu_x - \mu_v)(\mu_y - \mu_x) > 0. \tag{A3}$$

The numerator can be rewritten as

$$\begin{aligned} &(\mu_y^n - \mu_v^n)(\mu_x^2 - \mu_v^2) - (\mu_x^n - \mu_v^n)(\mu_y^2 - \mu_v^2) \\ &\quad = (\mu_y - \mu_v)\left(\sum_{k=1}^{n} \mu_y^{n-k}\mu_v^{k-1}\right)(\mu_x - \mu_v)(\mu_x + \mu_v) + (\mu_x - \mu_v)\left(\sum_{k=1}^{n} \mu_x^{n-k}\mu_v^{k-1}\right)(\mu_y - \mu_v)(\mu_y + \mu_v) \\ &\quad = (\mu_x - \mu_v)(\mu_y - \mu_v)\sum_{k=1}^{n} \left[(\mu_x + \mu_v)\mu_y^{n-k}\mu_v^{k-1} + (\mu_y - \mu_v)\mu_x^{n-k}\mu_v^{k-1}\right] \\ &\quad = (\mu_x - \mu_v)(\mu_y - \mu_v)\sum_{k=1}^{n} \left[(\mu_x\mu_y^{n-k} - \mu_y\mu_x^{n-k})\mu_v^{k-1} + (\mu_y^{n-k} - \mu_x^{n-k})\mu_v^{k}\right] \\ &\quad = (\mu_x - \mu_v)(\mu_y - \mu_v)\left\{\sum_{k=1}^{n-2} \left[\mu_x\mu_y(\mu_y^{n-k-1} - \mu_x^{n-k-1})\mu_v^{k-1} + (\mu_y^{n-k} - \mu_x^{n-k})\mu_v^{k}\right]\right. \\ &\qquad \left. + (\mu_y - \mu_x)\mu_v^{n-1} + (\mu_x - \mu_y)\mu_v^{n-1}\right\} \\ &\quad = (\mu_x - \mu_v)(\mu_y - \mu_v)\sum_{k=1}^{n-2} \left[\mu_x\mu_y(\mu_y^{n-k-1} - \mu_x^{n-k-1})\mu_v^{k-1} + (\mu_y^{n-k} - \mu_x^{n-k})\mu_v^{k}\right] \\ &\quad \geqslant 0, \qquad \text{when } n \geqslant 3. \end{aligned} \tag{A4}$$

The counting rate of any state must be non-negative, i.e. $\langle s_{0n} \rangle \geqslant 0$. Thus, we can conclude that $\xi_1 \geqslant 0$.

Appendix B. Formulas for the special case with asymmetric μ_v

In this case, we denote Alice's and Bob's intensities as $\mu_{v\mathrm{A}}$ and $\mu_{v\mathrm{B}}$, respectively, and the probabilities of n photons of Alice's and Bob's sources v as v_n^{A} and v_n^{B}, respectively. Formulas of the decoy-state analysis are

$$\langle s_{01}\rangle^{\mathrm{L}} = \frac{v_0^{\mathrm{B}}[(y_2v_0^{\mathrm{B}} - y_0v_2^{\mathrm{B}})\langle s_{0x}\rangle^{\mathrm{L}} - (x_2v_0^{\mathrm{B}} - x_0v_2^{\mathrm{B}})\langle s_{0y}\rangle^{\mathrm{U}} - (y_2x_0 - y_0x_2)\langle s_{0v}\rangle^{\mathrm{U}}]}{(y_2v_0^{\mathrm{B}} - y_0v_2^{\mathrm{B}})(x_1v_0^{\mathrm{B}} - x_0v_1^{\mathrm{B}}) - (x_2v_0^{\mathrm{B}} - x_0v_2^{\mathrm{B}})(y_1v_0^{\mathrm{B}} - y_0v_1^{\mathrm{B}})}, \tag{B1}$$

$$\langle s_{10}\rangle^{\mathrm{L}} = \frac{v_0^{\mathrm{A}}[(y_2v_0^{\mathrm{A}} - y_0v_2^{\mathrm{A}})\langle s_{x0}\rangle^{\mathrm{L}} - (x_2v_0^{\mathrm{A}} - x_0v_2^{\mathrm{A}})\langle s_{y0}\rangle^{\mathrm{U}} - (y_2x_0 - y_0x_2)\langle s_{v0}\rangle^{\mathrm{U}}]}{(y_2v_0^{\mathrm{A}} - y_0v_2^{\mathrm{A}})(x_1v_0^{\mathrm{A}} - x_0v_1^{\mathrm{A}}) - (x_2v_0^{\mathrm{A}} - x_0v_2^{\mathrm{A}})(y_1v_0^{\mathrm{A}} - y_0v_1^{\mathrm{A}})}, \tag{B2}$$

$$\langle s_{0v}\rangle^{\mathrm{U}} = \frac{1}{v_0^{\mathrm{A}}}\langle S_{vv}\rangle - \frac{v_1^{\mathrm{A}}v_0^{\mathrm{B}}}{v_0^{\mathrm{A}}}\langle s_{10}\rangle^{\mathrm{L}}, \tag{B3}$$

$$\langle s_{v0}\rangle^{\mathrm{U}} = \frac{1}{v_0^{\mathrm{B}}}\langle S_{vv}\rangle - \frac{v_1^{\mathrm{B}}v_0^{\mathrm{A}}}{v_0^{\mathrm{B}}}\langle s_{01}\rangle^{\mathrm{L}}, \tag{B4}$$

$$\langle s_{0y}\rangle^{\mathrm{U}} = \frac{1}{v_0^{\mathrm{A}}}\langle S_{vy}\rangle - \frac{v_1^{\mathrm{A}}y_0}{v_0^{\mathrm{A}}}\langle s_{10}\rangle^{\mathrm{L}}, \tag{B5}$$

$$\langle s_{y0}\rangle^{\mathrm{U}} = \frac{1}{v_0^{\mathrm{B}}}\langle S_{yv}\rangle - \frac{v_1^{\mathrm{B}}y_0}{v_0^{\mathrm{B}}}\langle s_{01}\rangle^{\mathrm{L}}, \tag{B6}$$

$$\langle s_{0x}\rangle^{\mathrm{L}} = \frac{x_1\langle S_{vx}\rangle - v_1^{\mathrm{A}}\langle S_{xx}\rangle}{x_1v_0^{\mathrm{A}} - x_0v_1^{\mathrm{A}}}, \tag{B7}$$

$$\langle s_{x0}\rangle^{\mathrm{L}} = \frac{x_1\langle S_{xv}\rangle - v_1^{\mathrm{B}}\langle S_{xx}\rangle}{x_1v_0^{\mathrm{B}} - x_0v_1^{\mathrm{B}}}. \tag{B8}$$

Combining equations (B1)–(B8), we can obtain

$$A_1\langle s_{01}\rangle^{\mathrm{L}} - B_1\langle s_{10}\rangle^{\mathrm{L}} = C_1 - D_1, \tag{B9}$$

$$A_2\langle s_{10}\rangle^{\mathrm{L}} - B_2\langle s_{01}\rangle^{\mathrm{L}} = C_2 - D_2, \tag{B10}$$

where we denote

$$\begin{aligned}
A_1 &= (\mu_y - \mu_{v\mathrm{B}})(\mu_x - \mu_{v\mathrm{B}})(\mu_y - \mu_x),\\
A_2 &= (\mu_y - \mu_{v\mathrm{A}})(\mu_x - \mu_{v\mathrm{A}})(\mu_y - \mu_x),\\
B_1 &= \mu_{v\mathrm{A}}(\mu_y^2 - \mu_{v\mathrm{B}}^2),\\
B_2 &= \mu_{v\mathrm{B}}(\mu_y^2 - \mu_{v\mathrm{A}}^2),\\
C_1 &= \mathrm{e}^{\mu_x+\mu_{v\mathrm{A}}}\frac{\mu_x}{\mu_x - \mu_{v\mathrm{A}}}(\mu_y^2 - \mu_{v\mathrm{B}}^2)\langle S_{vx}\rangle,\\
C_2 &= \mathrm{e}^{\mu_x+\mu_{v\mathrm{B}}}\frac{\mu_x}{\mu_x - \mu_{v\mathrm{B}}}(\mu_y^2 - \mu_{v\mathrm{A}}^2)\langle S_{xv}\rangle,\\
D_1 &= \mathrm{e}^{2\mu_x}\frac{\mu_{v\mathrm{A}}}{\mu_x - \mu_{v\mathrm{A}}}(\mu_y^2 - \mu_{v\mathrm{B}}^2)\langle S_{xx}\rangle + \mathrm{e}^{\mu_y+\mu_{v\mathrm{A}}}(\mu_x^2 - \mu_{v\mathrm{B}}^2)\langle S_{vy}\rangle + \mathrm{e}^{\mu_{v\mathrm{A}}+\mu_{v\mathrm{B}}}(\mu_y^2 - \mu_x^2)\langle S_{vv}\rangle,\\
D_2 &= \mathrm{e}^{2\mu_x}\frac{\mu_{v\mathrm{B}}}{\mu_x - \mu_{v\mathrm{B}}}(\mu_y^2 - \mu_{v\mathrm{A}}^2)\langle S_{xx}\rangle + \mathrm{e}^{\mu_y+\mu_{v\mathrm{B}}}(\mu_x^2 - \mu_{v\mathrm{A}}^2)\langle S_{yv}\rangle + \mathrm{e}^{\mu_{v\mathrm{A}}+\mu_{v\mathrm{B}}}(\mu_y^2 - \mu_x^2)\langle S_{vv}\rangle.
\end{aligned}$$

With equations (B9) and (B10), the lower bound of $\langle s_{01}\rangle$ and $\langle s_{10}\rangle$ can be calculated:

$$\langle s_{01}\rangle^{\mathrm{L}} = \frac{(A_2C_1 + B_1C_2) - (A_2D_1 + B_1D_2)}{A_1A_2 - B_1B_2}, \tag{B11}$$

$$\langle s_{10}\rangle^{\mathrm{L}} = \frac{(B_2C_1 + A_1C_2) - (B_2D_1 + A_1D_2)}{A_1A_2 - B_1B_2}, \tag{B12}$$

if $A_1A_2 - B_1B_2 > 0$. Then, the lower bound of $\langle s_{\mathrm{u}}\rangle$ is

$$\langle s_{\mathrm{u}}\rangle^{\mathrm{L}} = \frac{\langle s_{01}\rangle^{\mathrm{L}} + \langle s_{10}\rangle^{\mathrm{L}}}{2} = \frac{S'_{+} - S'_{-}}{2}, \tag{B13}$$

where

$$S'_{+} = \frac{A_2 + B_2}{A_1A_2 - B_1B_2}C_1 + \frac{A_1 + B_1}{A_1A_2 - B_1B_2}C_2, \tag{B14}$$

and

$$S'_{-}=\frac{A_2+B_2}{A_1A_2-B_1B_2}D_1+\frac{A_1+B_1}{A_1A_2-B_1B_2}D_2. \tag{B15}$$

If $A_1A_2-B_1B_2\leqslant 0$, $\langle s_{01}\rangle^{\mathrm{L}}=\langle s_{10}\rangle^{\mathrm{L}}=\langle s_{\mathrm{u}}\rangle^{\mathrm{L}}=0$ and thus no final key will be obtained. The lower bound of the expected number of the untagged bits is:

$$\langle n_{\mathrm{u}}\rangle^{\mathrm{L}}=\begin{cases}2N_Z\epsilon(1-\epsilon)v_0^{\mathrm{A}}z_1\langle s_{\mathrm{u}}\rangle^{\mathrm{L}} & \text{if } \mu_{v\mathrm{A}}\geqslant\mu_{v\mathrm{B}}\\ 2N_Z\epsilon(1-\epsilon)v_0^{B}z_1\langle s_{\mathrm{u}}\rangle^{\mathrm{L}} & \text{if } \mu_{v\mathrm{A}}<\mu_{v\mathrm{B}}\end{cases}. \tag{B16}$$

In calculation of the phase-flip error rate, we have

$$\langle s_{00}\rangle^{\mathrm{L}}=\begin{cases}\mathrm{e}^{\mu_{v\mathrm{A}}+\mu_{v\mathrm{B}}}\dfrac{\mu_x}{\mu_x-\mu_{v\mathrm{A}}}\langle S_{vv}\rangle-\mathrm{e}^{2\mu_x}\dfrac{\mu_{v\mathrm{A}}}{\mu_x-\mu_{v\mathrm{A}}}\langle S_{xx}\rangle & \text{if } \mu_{v\mathrm{A}}\geqslant\mu_{v\mathrm{B}}\\ \mathrm{e}^{\mu_{v\mathrm{A}}+\mu_{v\mathrm{B}}}\dfrac{\mu_x}{\mu_x-\mu_{v\mathrm{B}}}\langle S_{vv}\rangle-\mathrm{e}^{2\mu_x}\dfrac{\mu_{v\mathrm{B}}}{\mu_x-\mu_{v\mathrm{B}}}\langle S_{xx}\rangle & \text{if } \mu_{v\mathrm{A}}<\mu_{v\mathrm{B}}\end{cases}, \tag{B17}$$

and thus

$$\langle e_{\mathrm{u}}^{\mathrm{ph}}\rangle^{\mathrm{U}}=\begin{cases}\dfrac{\langle T_{X_1}\rangle+\frac{\mu_{v\mathrm{A}}}{2(\mu_x-\mu_{v\mathrm{A}})}\langle S_{xx}\rangle-\mathrm{e}^{\mu_{v\mathrm{A}}+\mu_{v\mathrm{B}}-2\mu_x}\frac{\mu_x}{2(\mu_x-\mu_{v\mathrm{A}})}\langle S_{vv}\rangle}{2\mu_x\,\mathrm{e}^{-2\mu_x}\langle s_{\mathrm{u}}\rangle^{\mathrm{L}}} & \text{if } \mu_{v\mathrm{A}}\geqslant\mu_{v\mathrm{B}}\\ \dfrac{\langle T_{X_1}\rangle+\frac{\mu_{v\mathrm{B}}}{2(\mu_x-\mu_{v\mathrm{B}})}\langle S_{xx}\rangle-\mathrm{e}^{\mu_{v\mathrm{A}}+\mu_{v\mathrm{B}}-2\mu_x}\frac{\mu_x}{2(\mu_x-\mu_{v\mathrm{B}})}\langle S_{vv}\rangle}{2\mu_x\,\mathrm{e}^{-2\mu_x}\langle s_{\mathrm{u}}\rangle^{L}} & \text{if } \mu_{v\mathrm{A}}<\mu_{v\mathrm{B}}\end{cases}. \tag{B18}$$

Appendix C. Related formulas for parameter estimation in AOPP

After obtaining the bounds of $\langle s_{01}\rangle$, $\langle s_{01}\rangle$, and $\langle e_{\mathrm{u}}^{\mathrm{ph}}\rangle$ in the decoy-state analysis, we can use the following related formulas to estimate the bounds of the number of the survived untagged bits after AOPP, n'_{u}.

$$u=\frac{n_g}{2n_{\mathrm{odd}}}, \tag{C1}$$

$$\langle n_{01}\rangle^{\mathrm{L}}=N_Z\epsilon(1-\epsilon)v_0z_1\langle s_{01}\rangle^{\mathrm{L}}, \tag{C2}$$

$$\langle n_{10}\rangle^{\mathrm{L}}=N_Z\epsilon(1-\epsilon)v_0z_1\langle s_{10}\rangle^{\mathrm{L}}, \tag{C3}$$

$$n_{01}^{\mathrm{L}}=O^{\mathrm{L}}(u\langle n_{01}\rangle^{\mathrm{L}},\xi), \tag{C4}$$

$$n_{10}^{\mathrm{L}}=O^{\mathrm{L}}(u\langle n_{10}\rangle^{\mathrm{L}},\xi), \tag{C5}$$

$$n_1^{\mathrm{L}}=n_{01}^{\mathrm{L}}+n_{10}^{\mathrm{L}}, \tag{C6}$$

$$n_1^{r}=O^{\mathrm{L}}\left(\frac{(n_1^{\mathrm{L}})^2}{2un_Z},\xi\right), \tag{C7}$$

$$n'_{01}=2n_1^{r}\left(\frac{n_{01}^{\mathrm{L}}}{n_1^{\mathrm{L}}}-\sqrt{-\frac{\ln\xi}{2n_1^{r}}}\right), \tag{C8}$$

$$n'_{10}=2n_1^{r}\left(\frac{n_{10}^{\mathrm{L}}}{n_1^{\mathrm{L}}}-\sqrt{-\frac{\ln\xi}{2n_1^{r}}}\right), \tag{C9}$$

$$n_{\min}=\min(n'_{01},n'_{10}), \tag{C10}$$

$$n_{\mathrm{u}}^{\prime\mathrm{L}}=2O^{\mathrm{L}}\left(n_{\min}\left(1-\frac{n_{\min}}{2n_1^{r}}\right),\xi\right), \tag{C11}$$

where n_Z is number of raw keys that Alice and Bob get in the experiment, i.e., the number of effective Z windows; n_g is the number of pair if Alice and Bob perform AOPP to their raw keys; n_{odd} is the number of pairs with odd-parity if Alice randomly groups all the bits in her raw keys two by two; n_Z, n_g, and n_{odd} are observed values; ξ is the failure probability of parameter estimation; and $O^{\mathrm{L}}(Y,\xi)$ is the lower bounds while using Chernoff bound [54], which is shown in equation (D6).

And the related formulas of $e_{\mathrm{u}}^{\prime\mathrm{ph}}$ are:

$$r = \frac{n_1^{\mathrm{L}}}{n_1^{\mathrm{L}} - 2n_1^r} \ln \frac{3(n_1^{\mathrm{L}} - 2n_1^r)^2}{\xi}, \tag{C12}$$

$$e_\tau = \frac{O^{\mathrm{U}}(2n_1^r \langle e_{\mathrm{u}}^{\mathrm{ph}} \rangle^{\mathrm{U}}, \xi)}{2n_1^r - r}, \tag{C13}$$

$$M_s = O^U\left[(n_1^r - r)e_\tau(1 - e_\tau), \xi\right] + r, \tag{C14}$$

$$(e_{\mathrm{u}}^{\prime \mathrm{ph}})^{\mathrm{U}} = \frac{2M_s}{n_{\mathrm{u}}^{\prime \mathrm{L}}}, \tag{C15}$$

where $O^{\mathrm{U}}(Y, \xi)$ is the upper bounds while using Chernoff bound, which is shown in equation (D5).

Appendix D. Chernoff bound

We can use the Chernoff bound to estimate the expected value with their observed values [54]. We denote $X_1, X_2, \ldots, X_n$ as n random samples, whose values are 1 or 0, and X as their sum satisfying $X = \sum_{i=1}^{n} X_i$. We denote E as the expected value of X. We have

$$E^{\mathrm{L}}(X, \xi) = \frac{X}{1 + \delta_1(X, \xi)}, \tag{D1}$$

$$E^{\mathrm{U}}(X, \xi) = \frac{X}{1 - \delta_2(X, \xi)}, \tag{D2}$$

where $\delta_1(X, \xi)$ and $\delta_2(X, \xi)$ are the positive solutions of the following equations:

$$\left(\frac{\mathrm{e}^{\delta_1}}{(1 + \delta_1)^{1+\delta_1}}\right)^{\frac{X}{1+\delta_1}} = \xi, \tag{D3}$$

$$\left(\frac{\mathrm{e}^{-\delta_2}}{(1 - \delta_2)^{1-\delta_2}}\right)^{\frac{X}{1-\delta_2}} = \xi, \tag{D4}$$

where ξ is the failure probability.

Besides, the Chernoff bound can be used to estimate their real values with their expected values. Similar to equations (D1)–(D4), the real value, O, can be estimated by its expected value, Y:

$$O^{\mathrm{U}}(Y, \xi) = [1 + \delta_1'(Y, \xi)]Y, \tag{D5}$$

$$O^{\mathrm{L}}(Y, \xi) = [1 - \delta_2'(Y, \xi)]Y, \tag{D6}$$

where $\delta_1'(Y, \xi)$ and $\delta_2'(Y, \xi)$ are the positive solutions of the following equations:

$$\left(\frac{\mathrm{e}^{\delta_1'}}{(1 + \delta_1')^{1+\delta_1'}}\right)^{Y} = \xi, \tag{D7}$$

$$\left(\frac{\mathrm{e}^{-\delta_2'}}{(1 - \delta_2')^{1-\delta_2'}}\right)^{Y} = \xi. \tag{D8}$$

Appendix E. Improvement in decoy-state analysis

To complete the calculation, they need observed values for expected values of some quantities at the right-hand side of equations (23), (24) and (37). If they choose to do the decoy-state analysis after error correction [58], they can make it more efficiently. As shown in reference [58], assisted by classical communications, they can actually know those observed numbers of all kinds of events. However, the announcement of some of these numbers (we name them as the confidential observed numbers) may cause information leakage such as n_{vz} and n_{zv}. Suppose Bob is the party who computes the positions of wrong bits. He does not announce these positions. He is able to use them and all the other kinds of observed numbers. For security, we need deduct a certain amount of bits from the final key. If Bob uses these values, he does not announce them directly. All information announced is the final key length, which is known to be upper bounded by $\tilde{N}$, i.e., the largest possible key length calculated from equation (6) if the decoy-state analysis is done before error correction or is not done. This means an additional mutual information between Eve and the key distilled from equation (6), upper bounded by $\log_2 \tilde{N}$ [47]. Theorem: if we use the following key length formula, Bob can use numbers of whatever kinds of events in decoy-state analysis after error correction:

$$N_{\mathrm{f}}^{(1)} = n'_{\mathrm{u}}[1 - H(e'^{\mathrm{ph}}_{\mathrm{u}})] - f n'_Z H(E'_Z) - 2\left(\log_2 \frac{2}{\varepsilon_{\mathrm{cor}}} - 2\log_2 \frac{1}{\sqrt{2}\varepsilon_{\mathrm{PA}}\hat{\varepsilon}}\right) - \log_2 \tilde{N}. \tag{E1}$$

There are many simple settings for the value of $\tilde{N}$. For example, we can use n'_z which is the number of bits to be distilled after AOPP, or a bit more tightly, $n'_z[1 - fH(E'_z)]$.

Specifically, the observed numbers such as n_{vx}, n_{xv}, n_{vy}, n_{yv}, n_{vv}, n_{vz}, n_{zv}, $n_{vz} + n_{zv}$, and n_{zz} can all be used for the decoy-state analysis of s_{01} and s_{10}. The values of n_{vx}, n_{vy}, n_{xv}, n_{yv}, n_{vv}, n_{xx} can be used to verify the value ranges of $\langle S_{vx}\rangle$, $\langle S_{vy}\rangle$, $\langle S_{xv}\rangle$, $\langle S_{yv}\rangle$, $\langle S_{vv}\rangle$, and $\langle S_{xx}\rangle$ used in the right-hand-side of equations (23), (24) and (25), and also $\langle S_{vz}\rangle$ and $\langle S_{zv}\rangle$ which are useful in a protocol with three intensities.

To formulate n_0 in equation (38) with imperfect vacuum, we introduce the definition of VA-pair similar to that in reference [58]: a bit pair made by Alice in AOPP, where both bits of Alice are from time windows when she has actually sent out state ρ_v. In our protocol, we request that Alice makes all those AOPP pairs and Bob computes the positions of wrong bits in error correction and corrects his wrong bits privately. Note that, although Eve and Bob know the parity of Alice's bits in a VA-pair, Eve and Bob have no idea on which bit in the VA-pair takes the bit value 0 or 1, since the quantum state sent out for both bits are identical (ρ_v). If we only take one bit from the VA-pair, the bit is completely Alice's private bit of which no one outside Alice's lab can have any information. Thus, a VA-pair survived through the parity check will contribute one secure bit for final key distillation. To make such VA-pairs, the state in time windows when Alice decides sending can be written in another convex form:

$$\rho(\mu_z) = z'_0\rho_v + \sum_{n=1}^{\infty} z'_n\rho_n, \tag{E2}$$

where $z'_0 = \mathrm{e}^{-\mu_z+\mu_v}$ and $z'_n = \mathrm{e}^{-\mu_z}(\mu_z^n - \mu_v^n)/n!$. Equation (E2) means that when Alice decides sending, she sends out ρ_v with a probability of z'_0 and ρ_n with a probability of z'_n. When calculating the number of untagged bits in equation (28), we have to replace z_1 by z'_1.

The value of n_0 can be calculated by the number of VA-pairs whose parity values at Bob's side are odd. Asymptotically,

$$n_0 = n_{\mathrm{A,not}}\frac{\epsilon}{1-\epsilon}z'_0 \cdot \eta_{\mathrm{odd}} \tag{E3}$$

if $n_{\mathrm{A,not}} \geqslant n_{\mathrm{A,S}}$, and

$$n_0 = \frac{n_{\mathrm{A,not}}}{n_{\mathrm{A,S}}} \cdot n_{\mathrm{A,not}}\frac{\epsilon}{1-\epsilon}z'_0 \cdot \eta_{\mathrm{odd}} \tag{E4}$$

if $n_{\mathrm{A,not}} < n_{\mathrm{A,S}}$, where $n_{\mathrm{A,S}}$ ($n_{\mathrm{A,not}}$) is the number of effective Z windows when Alice decides sending (not-sending), and η_{odd} is the probability that the parity value at Bob's side of a VA-pair is odd. To obtain η_{odd}, Bob can directly make pairs with all those Alice's not-sending bits from effective Z windows, make deterministic VA-pairs based on these, and observe the rate of odd parity at his own side and hence verify the value of η_{odd}. The non-asymptotic result of n_0 can be obtained by using Chernoff bound and the hypergeometric distribution model.

ORCID iDs

Xiang-Bin Wang https://orcid.org/0000-0002-3026-9364

References

[1] Bennett C H and Brassard G 1984 *Proc. of the IEEE Int. Conf. on Computers, Systems, and Signal Processing* pp 175–9
[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[3] Xu F, Ma X, Zhang Q, Lo H-K and Pan J-W 2020 *Rev. Mod. Phys.* **92** 025002
[4] Pirandola S *et al* 2020 *Adv. Opt. Photon.* **12** 1012
[5] Hwang W-Y 2003 *Phys. Rev. Lett.* **91** 057901
[6] Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503
[7] Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[8] Lo H-K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[9] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[10] Rubenok A, Slater J A, Chan P, Lucio-Martinez I and Tittel W 2013 *Phys. Rev. Lett.* **111** 130501
[11] Liu Y *et al* 2013 *Phys. Rev. Lett.* **111** 130502

[12] 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. Photon.* **10** 312
[13] Wang C, Yin Z-Q, Wang S, Chen W, Guo G-C and Han Z-F 2017 *Optica* **4** 1016
[14] Semenenko H, Sibson P, Hart A, Thompson M G, Rarity J G and Erven C 2020 *Optica* **7** 238
[15] Wei K *et al* 2020 *Phys. Rev.* X **10** 031030
[16] Zheng X *et al* 2021 *Adv. Photon.* **3** 055002
[17] Yin H-L *et al* 2016 *Phys. Rev. Lett.* **117** 190501
[18] Zhou Y-H, Yu Z-W and Wang X-B 2016 *Phys. Rev.* A **93** 042324
[19] Hu X L, Jiang C, Yu Z W and Wang X B 2021 *Adv. Quantum Technol.* **4** 2100069
[20] Yu Z-W, Zhou Y-H and Wang X-B 2015 *Phys. Rev.* A **91** 032318
[21] Xu F, Xu H and Lo H-K 2014 *Phys. Rev.* A **89** 052333
[22] Boaron A *et al* 2018 *Phys. Rev. Lett.* **121** 190502
[23] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 15043
[24] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[25] Minder M, Pittaluga M, Roberts G L, Lucamarini M, Dynes J F, Yuan Z L and Shields A J 2019 *Nat. Photon.* **13** 334
[26] Liu Y *et al* 2019 *Phys. Rev. Lett.* **123** 100505
[27] Wang S, He D-Y, Yin Z-Q, Lu F-Y, Cui C-H, Chen W, Zhou Z, Guo G-C and Han Z-F 2019 *Phys. Rev.* X **9** 021046
[28] Zhong X, Hu J, Curty M, Qian L and Lo H-K 2019 *Phys. Rev. Lett.* **123** 100506
[29] Chen J-P *et al* 2020 *Phys. Rev. Lett.* **124** 070501
[30] Liu H *et al* 2021 *Phys. Rev. Lett.* **126** 250502
[31] Chen J-P *et al* 2021 *Nat. Photon.* **15** 570
[32] Pittaluga M, Minder M, Lucamarini M, Sanzaro M, Woodward R I, Li M-J, Yuan Z and Shields A J 2021 *Nat. Photon.* **15** 530
[33] Clivati C *et al* 2022 *Nat. Commun.* **13** 1
[34] Wang S *et al* 2022 *Nat. Photon.* **16** 154
[35] Chen J-P *et al* 2022 *Phys. Rev. Lett.* **128** 180502
[36] Wang X-B, Yu Z-W and Hu X-L 2018 *Phys. Rev.* A **98** 062323
[37] Yu Z-W, Hu X-L, Jiang C, Xu H and Wang X-B 2019 *Sci. Rep.* **9** 3080
[38] Jiang C, Yu Z-W, Hu X-L and Wang X-B 2019 *Phys. Rev. Appl.* **12** 024061
[39] Hu X-L, Jiang C, Yu Z-W and Wang X-B 2019 *Phys. Rev.* A **100** 062337
[40] Xu H, Yu Z-W, Jiang C, Hu X-L and Wang X-B 2020 *Phys. Rev.* A **101** 042330
[41] Jiang C, Hu X-L, Xu H, Yu Z-W and Wang X-B 2020 *New J. Phys.* **22** 053048
[42] Jiang C, Hu X-L, Yu Z-W and Wang X-B 2021 *New J. Phys.* **23** 063038
[43] Song T, Li P and Weng J 2021 *Phys. Rev.* A **103** 042408
[44] Teng J *et al* 2021 *Phys. Rev.* A **104** 062441
[45] Hu X-L, Zhou Y-H, Yu Z-W and Wang X-B 2017 *Phys. Rev.* A **95** 032331
[46] Hu X-L, Yu Z-W and Wang X-B 2018 *Phys. Rev.* A **98** 032303
[47] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634
[48] Curty M, Xu F, Cui W, Lim C C W, Tamaki K and Lo H-K 2014 *Nat. Commun.* **5** 1–7
[49] Lim C C W, Curty M, Walenta N, Xu F and Zbinden H 2014 *Phys. Rev.* A **89** 022307
[50] Wang Y, Bao W-S, Zhou C, Jiang M-S and Li H-W 2016 *Phys. Rev.* A **94** 032335
[51] Wang Y, Bao W-S, Zhou C, Jiang M-S and Li H-W 2019 *J. Opt. Soc. Am.* B **36** B83
[52] Inamori H, Lütkenhaus N and Mayers D 2007 *Eur. Phys. J.* D **41** 599
[53] Gottesman D, Lo H-K, Lutkenhaus N and Preskill J 2004 *Int. Symp. on Information Theory, 2004. ISIT 2004. Proc.* (IEEE) p 136
[54] Chernoff H 1952 *Ann. Math. Stat.* **23** 493
[55] Jiang C, Yu Z-W, Hu X-L and Wang X-B 2021 *Phys. Rev.* A **103** 012402
[56] Chau H 2020 *Phys. Rev.* A **102** 012611
[57] Lo H-K 2005 *Quantum Inf. Comput.* **5** 413
[58] Hu X-L, Jiang C, Yu Z-W and Wang X-B 2022 arXiv:2204.12890