Security of the BB84 protocol with passive biased basis choice by the receiver

Shun Kawakami,[1,2,*] Atsushi Taniguchi,[1] Yoshihide Tonomura,[1] Koichi Takasugi,[1] and Koji Azuma[3,2]

[1] *Network Innovation Laboratories, NTT Inc., 1-1 Hikari-no-oka, Yokosuka, Kanagawa 239-0847, Japan*

[2] *NTT Research Center for Theoretical Quantum Information, NTT Inc., 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

[3] *Basic Research Laboratories, NTT Inc., 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

(Received 31 July 2025; revised 10 October 2025; accepted 17 October 2025; published 24 November 2025)

The Bennett-Brassard 1984 (BB84) protocol is one of the simplest protocols for implementing quantum key distribution (QKD). In the protocol, the sender and the receiver iteratively choose one of two complementary measurement bases. Regarding the basis choice by the receiver, a passive setup has been adopted in a number of its implementations, including satellite QKD and time-bin encoding. However, conventional theoretical techniques to prove the security of the BB84 protocol are not applicable if the receiver chooses their measurement basis passively, rather than actively, with a biased probability, followed by measurement with threshold detectors. Here we present a fully analytical security proof against coherent attacks for such a decoy-state BB84 protocol with the receiver's passive basis choice and measurement with threshold detectors. Numerical simulations under practical situations show that the difference in secure key rate between the active and passive implementations of the protocol is negligible except for long communication distances.

DOI: 10.1103/2pzb-ssrs

I. INTRODUCTION

Quantum key distribution (QKD) is an established research field among a number of quantum information processing technologies from the perspective of both theory and implementation. Many QKD protocols have been proposed so far, but the Bennett-Brassard 1984 (BB84) protocol [1] is one of the most frequently demonstrated protocols, and its security analysis has been well studied. Although the sender is assumed to emit a single photon in the ideal BB84 protocol, in practice weak coherent pulses can be used instead with the decoy-state method [2–5], in which the pulse intensities are modulated, to estimate the contribution of single-photon emission to key generation. Regarding the receiver, although a single photon is assumed to be received in the ideal BB84 protocol, the arrival of a single photon cannot be distinguished from that of multiple photons because threshold (or on-off) detectors are used in practice. Nevertheless, the security of such a decoy-state BB84 protocol implemented with threshold detectors is proven thanks to sophisticated theoretical techniques such as the squashing method [6,7] and security proofs with complementarity [8,9] and with the entropic uncertainty relation [10].

In the conventional practical BB84 protocol, the sender and the receiver actively choose one of two complementary bases, called Z basis and X basis, with a certain probability, perhaps with a biased one to achieve a higher key rate [11]. We call such a biased choice the "active biased BB84" protocol. On the other hand, from the perspective of implementation, a passive basis choice by the receiver, in which a single beam splitter is set to split the incoming light into two passes corresponding to the bases, is a realistic option especially in satellite-based QKD with polarization encoding [12–15] and the time-bin phase encoding BB84 protocol [16–20]. For this kind of receiver's passive setup, a basis choice with an unbalanced probability is worth considering in order not only to achieve a higher key generation rate but also to relax the required absolute precision in the splitting ratio of 50:50 of the beam splitter used for the unbiased basis choice. However, the above theoretical techniques for the BB84 protocol with threshold detectors cannot directly be applied to such a "passive biased BB84" protocol. For the passive biased BB84 protocol, a squashing map does not exist [21]. Furthermore, the security proof with complementarity as well as with the entropic uncertainty relation can be applied to

*Contact author: shun.kawakami@ntt.com

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

the passive protocol only if the basis choice is balanced [22] (as explicitly shown below with Appendix A).

Recently, the security of the decoy-state QKD protocol with passive biased basis choice has been proved [21] by using a flag-state squasher [23], in which an infinite photon-number space is analytically squashed to a finite photon-number space so as to numerically solve an optimization problem in the finite space. However, their proof has been based on the "IID assumption," i.e., the quantum states shared between the sender and the receiver after interference by an eavesdropper have been assumed to be independent and identically distributed among all rounds of the protocol, until very recently [24,25]. Besides, compared with conventional analytic approaches [8–10], this type of numerical approach necessitates an additional workload to calculate the amount of privacy amplification needed from the observed data in the quantum phase of the protocol, before entering the classical postprocessing phase.

In this paper, in contrast, we present a fully analytical security proof of the decoy-state BB84 protocol with the receiver's passive biased basis choice against coherent attacks in the asymptotic regime. This is done by applying the security proof for the BB84 protocol with complementarity [8,9], which inherently covers coherent attacks, *only* to the single-photon subspace at the receiver. Our proof explicitly gives the key generation rate including the effect of dark counts and asymmetric loss between two bases. Our work shows that the difference in key generation rate between the active biased and the passive biased BB84 protocols is negligible except for the range of long distances where the dark count rate of detectors is relevant to the key rate. This implies that the passive setup of the receiver does not sacrifice the efficiency in key generation despite its implementational benefits.

This paper is organized as follows. In Sec. II, we describe the BB84 protocol with the receiver's passive basis choice and assumptions on apparatus. Section III gives the security proof of the protocol, and shows a formula for the key rate. In Sec. IV, numerical results are shown and compared with the active protocol. Section V gives conclusions.

II. PROTOCOL AND ASSUMPTIONS

Here we introduce a polarization-type BB84 protocol with the decoy-state method where the receiver selects their basis passively. The sender is called Alice and the receiver is called Bob. In the protocol, two complementary bases (Z and X) are used to generate nonorthogonal states where the secret key is extracted from the Z basis and the signal disturbance is monitored in the X basis. The protocol is described as follows.

(1) *State preparation.* Alice chooses her bit $b_A \in \{0,1\}$ at random and basis $W_A \in \{Z,X\}$ with probability p_{W_A} ($p_Z \geq p_X$, $p_Z + p_X = 1$) to determine a polarization $P \in \{H,V,D,\bar{D}\}$, where $P = H$, V, D, and $\bar{D}$ are chosen when $(W_A, b_A) = (Z,0)$, $(Z,1)$, $(X,0)$, and $(X,1)$, respectively. She chooses intensity $\mu_A \in \{\mu,\nu,0\}$ ($\mu > \nu > 0$) with probability p_{μ_A} ($p_\mu + p_\nu + p_0 = 1$). She also chooses phase $\delta_A \in [0,2\pi)$ at random, which will never be revealed. Accordingly, she prepares a perfect coherent state

$$|\alpha_P\rangle_{A'} := e^{-\mu_A/2} \sum_{n_A \geq 0} \frac{(\sqrt{\mu_A}\, e^{i\delta_A} \hat{a}_P^\dagger)^{n_A}}{n_A!} |\mathrm{vac}\rangle_{A'}, \quad (1)$$

where $|\mathrm{vac}\rangle_{A'}$ represents the vacuum state and $\hat{a}_P^\dagger$ is the creation operator of polarization $P \in \{H,V,D,\bar{D}\}$ satisfying $\hat{a}_D^\dagger = (\hat{a}_H^\dagger + \hat{a}_V^\dagger)/\sqrt{2}$ and $\hat{a}_{\bar{D}}^\dagger = (\hat{a}_H^\dagger - \hat{a}_V^\dagger)/\sqrt{2}$. Alice sends the coherent state to Bob. Since δ_A is chosen at random and is never revealed, her state is regarded as a mixture of Fock states,

$$\frac{1}{2\pi} \int_0^{2\pi} |\alpha_P\rangle_{A'} \langle\alpha_P|\, d\delta_A = \sum_{n_A \geq 0} P_{\mu_A}^{\mathrm{Poisson}}(n_A)\, |P^{(n_A)}\rangle_{A'} \langle P^{(n_A)}|, \quad (2)$$

where $P_{\mu_A}^{\mathrm{Poisson}}(n_A) := e^{-\mu_A} \mu_A^{n_A}/n_A!$ ($\mu_A \in \{\mu,\nu,0\}$) is a Poisson distribution and $|P^{(n_A)}\rangle_{A'} := (\hat{a}_P^\dagger)^{n_A}/\sqrt{n_A!}\, |\mathrm{vac}\rangle_{A'}$ is an n_A-photon-number state with a polarization $P \in \{H,V,D,\bar{D}\}$.

(2) *Measurement.* With the linear optical setup in Fig. 1, Bob passively splits an incoming signal to the "Z line" and "X line" to perform Z-basis measurement and X-basis measurement, respectively, with splitting ratio $p_Z : p_X$ by using a beam splitter (BS). In the X line, a half-wave plate (HWP), whose transmittance might be smaller than unity, is set to rotate the polarization by 45°. In both lines, a polarization beam splitter (PBS) splits the pass depending on whether the polarization is horizontal or vertical. Four threshold detectors have a dark-count probability $0 \leq d \leq 1$ per pulse. In the Z (X) line, two detectors have an identical quantum efficiency η_{det}^Z (η_{det}^X) and the overall transmittance of the line, including the quantum efficiency, is η_Z (η_X), satisfying $0 \leq \eta_X \leq \eta_Z \leq 1$ (as the X line may have additional optical components such as a half-wave plate). Now define a parameter

$$r := \frac{\eta_X}{\eta_Z} \ (\leq 1), \quad (3)$$

representing the asymmetric transmittance between the two lines. Bob registers $y_B = 1$ if at least one of the four detectors clicks, and $y_B = 0$ if no detector clicks. If $y_B = 1$ and no detection occurs in the X (Z) line, he regards his measurement basis as $W_B = Z$ (X). If there is a "double click" despite $W_B \in \{Z,X\}$, in which both detectors

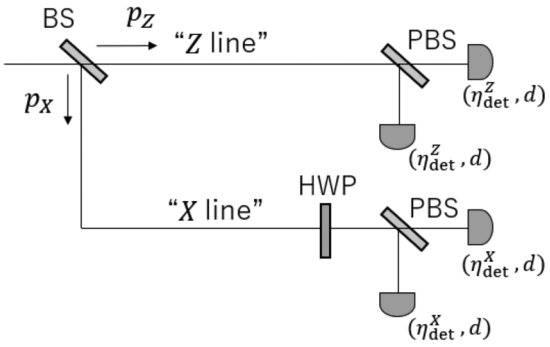


FIG. 1. Bob's actual setup for passive basis choice with a beam splitter (BS), polarization beam splitters (PBSs), a half-wave plate (HWP), and threshold detectors. Incoming light is split into the Z line or X line with the ratio of $p_Z : p_X$. All detectors have identical dark count probability d. The quantum efficiencies of detectors in the Z line and X line are $\eta_{\rm det}^Z$ and $\eta_{\rm det}^X$, respectively. The overall transmittances, including the quantum efficiency, in the Z line and X line are η_Z and η_X, respectively $(\eta_Z \geq \eta_X)$.

announce the arrival of photon in a single line, he assigns a bit value 0 or 1 at random to his bit b_B, but otherwise he determines $b_B \in \{0,1\}$ depending on which detector clicks. If $y_B = 1$ but there is a "cross click" corresponding to multiple detections across the two lines, he regards the round as $W_B = \perp$ and does not assign any bit.

(3) *Repetition.* Alice and Bob repeat steps (1) and (2) $m_{\rm rep}$ times.

(4) *Public communication.* For all $m_{\rm rep}$ rounds, Alice and Bob publicly announce y_B, W_A, W_B, and μ_A. They also disclose b_A for a round with $W_A = X$ and b_B for a round with $W_B = X$.

(5) *Basis reconciliation.* From rounds with $y_B = 1$, $W_A = Z$, and $W_B = Z$, Alice and Bob randomly extract $m_{\rm sam}$ sample rounds and disclose their bits b_A and b_B to calculate the bit error rate e_Z. Let $m_{\rm gen} := m_{\rm rep} - m_{\rm sam}$ be the number of all rounds removing rounds for the sampling, called nonsampling rounds. Hereafter we use the notation $m(\Omega = \omega)$ as the number of nonsampling rounds where a condition $\Omega = \omega$ is satisfied. Alice and Bob obtain a bit sequence with length $m_{W,\mu'} := m(y_B = 1 \wedge W_A = W_B = W \wedge \mu_A = \mu')$ for $W \in \{Z,X\}$ and $\mu' \in \{\mu,\nu,0\}$. For the Z basis, they generate a sifted key with length $m_Z := m_{Z,\mu} + m_{Z,\nu} + m_{Z,0}$. For the X basis, they obtain the number of bit errors, $m_{X,\mu'}^{\rm error} := m(y_B = 1 \wedge W_A = W_B = X \wedge \mu_A = \mu' \wedge b_A \neq b_B)$, for each of $\mu' \in \{\mu,\nu,0\}$. They obtain the number of cross clicks, $m_{{\rm cross},\mu'} := m(y_B = 1 \wedge W_B = \perp \wedge \mu_A = \mu')$, for each of $\mu' \in \{\mu,\nu,0\}$. They also obtain the number $m_{\mu'} := m(\mu_A = \mu')$ for $\mu' \in \{\mu,\nu,0\}$.

(6) *Error correction.* Alice generates a syndrome of length $m_{\rm gen} f_{\rm EC}$ depending on the bit error rate e_Z from her sifted key. She encrypts it by consuming a preshared key with Bob and sends it to him [8]. Bob corrects his key based on the decrypted syndrome.

(7) *Privacy amplification.* Alice and Bob conduct privacy amplification by shortening their keys by $m_{\rm gen} f_{\rm PA}$ bits to obtain a final key.

Let us define the following ratios by using the numbers appearing in the above protocol:

$$Q_Z := \frac{m_Z}{m_{\rm gen}}, \qquad Q_{Z|\mu_A} := \frac{m_{Z,\mu_A}}{m_{\mu_A}},$$
$$E_{X|\mu_A} := \frac{m_{X,\mu_A}^{\rm error}}{m_{\mu_A}}, \quad Q_{{\rm cross}|\mu_A} := \frac{m_{{\rm cross},\mu_A}}{m_{\mu_A}}. \tag{4}$$

In this paper, we consider the asymptotic secure key rate in the limit of $m_{\rm rep} \to \infty$. In this limit, the asymptotic value of $f_{\rm PA}$ is expressed as a function of $\{Q_{Z|\mu_A}, E_{X|\mu_A}, Q_{{\rm cross}|\mu_A}\}_{\mu_A \in \{\mu,\nu,0\}}$. The key rate R per nonsampling round is given by

$$R = Q_Z - f_{\rm PA}(\{Q_{Z|\mu_A}, E_{X|\mu_A}, Q_{{\rm cross}|\mu_A}\}_{\mu_A \in \{\mu,\nu,0\}}) - f_{\rm EC}. \tag{5}$$

III. SECURITY PROOF

The difficulty of the security proof for the passive biased BB84 protocol stems from the fact that the probability of Bob's basis choice depends on the photon number (n_B) contained in an incoming signal. More details of the theoretical difference between the active and the passive basis choices are shown in Appendix A. Our approach to overcome this difficulty is to focus on rounds with $n_B = 1$ to fix the probability of Bob's basis choice, which enables the proof to be reduced to that of the active basis choice. As the proof for the active basis choice, we adopt the security proof with complementarity [8,9]. To realize this scenario, the rounds where Alice emits no less than a single photon and Bob receives multiple photons $(n_A \geq 1 \wedge n_B \geq 2)$ are considered to be insecure in our proof. To estimate the contribution of multiple-photon detection to key generation, we use the observed number of cross clicks [21].

A. Alternative protocol

Our starting point is to introduce an alternative protocol, which is equivalent to the actual protocol from the viewpoint of an eavesdropper called Eve. The alternative protocol is described by replacing the steps (1) and (2) in the actual protocol to the following.

(1′) *State preparation.* Alice first chooses a photon number n_A according to the Poisson distribution $P_{\mu_A}^{\rm Poisson}(n_A)$ and chooses her basis $W_A \in \{Z,X\}$ with probability p_{W_A}. She prepares $|\Phi_Z^{(n_A)}\rangle_{AA'}$, followed by the projective measurement $\{|0\rangle\langle 0|_A, |1\rangle\langle 1|_A\}$ for the Z basis on system A to obtain the outcome b_A, or prepares $|\Phi_X^{(n_A)}\rangle_{AA'}$, followed by

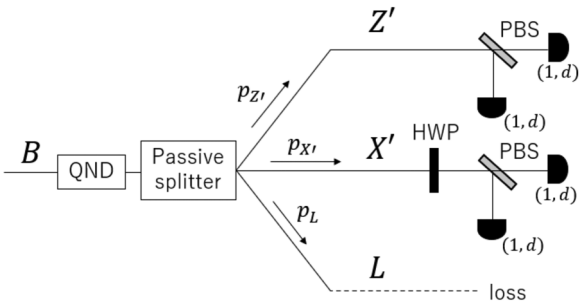


FIG. 2. Bob's virtual setup equivalent to the actual setup shown in Fig. 1. The QND measurement is conducted to obtain the photon number n_B. The incoming light is split into the Z', X', and L lines with the ratio of $p_{Z'} := p_Z$, $p_{X'} := p_X r$, and $p_L := 1 - p_{Z'} - p_{X'}$, respectively, where $r = \eta_X/\eta_Z$. The L line represents photon loss, while the Z' and X' lines are lossless. All threshold detectors in the Z' and X' lines have the quantum efficiency 1 and dark count probability d.

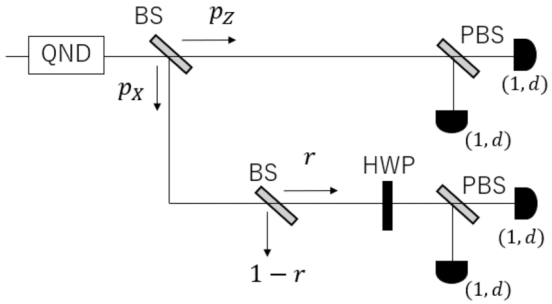


FIG. 3. Bob's virtual setups connecting Figs. 1 and 2. The QND measurement is conducted to obtain the photon number n_B. The common transmittance η_Z between the Z and X lines in Fig. 1 is absorbed in the quantum channel. The transmittance in the Z line is 1 and that in the X line is $r = \eta_X/\eta_Z$, modeled as a BS in the figure. All threshold detectors have the quantum efficiency of 1 and dark-count probability d.

the projective measurement $\{|+\rangle\langle+|_A, |-\rangle\langle-|_A\}$ for the X basis, where

$$\begin{aligned} |\Phi_Z^{(n_A)}\rangle_{AA'} &:= (|0\rangle_A |H^{(n_A)}\rangle_{A'} + |1\rangle_A |V^{(n_A)}\rangle_{A'})/\sqrt{2}, \\ |\Phi_X^{(n_A)}\rangle_{AA'} &:= (|+\rangle_A |D^{(n_A)}\rangle_{A'} + |-\rangle_A |\bar{D}^{(n_A)}\rangle_{A'})/\sqrt{2}, \end{aligned} \tag{6}$$

and $\{|0\rangle_A, |1\rangle_A\}$ is a computational basis with $|\pm\rangle_A := (|0\rangle_A \pm |1\rangle_A)/\sqrt{2}$. Alice sends system A' to Bob. Note that, for $n_A = 1$,

$$|\Phi_Z^{(1)}\rangle_{AA'} = |\Phi_X^{(1)}\rangle_{AA'} \tag{7}$$

holds, which implies that Alice prepares the same state independently of her basis choice, and thus her measurement on system A can be postponed until the signal arrives at Bob's site. For $n_A = 0$, since we have $|P^{(0)}\rangle_{A'} = |\text{vac}\rangle_{A'}$ for any $P \in \{H, V, D, \bar{D}\}$,

$$|\Phi_Z^{(0)}\rangle_{AA'} = |+\rangle_A |\text{vac}\rangle_{A'} \tag{8}$$

holds.

(2′) *Measurement.* As shown in Fig. 2, Bob conducts a polarization-independent quantum nondemolition (QND) measurement to obtain the photon number n_B. He then passively splits the incoming light into three passes to the Z' line, X' line, and L line with the splitting ratio of $p_{Z'} := p_Z$, $p_{X'} := p_X r$, and $p_L := 1 - p_{Z'} - p_{X'}$, respectively, where the Z' and X' lines are lossless and have detectors with quantum efficiency 1 and dark count probability d per pulse, while all photons in the L line are lost.

We explain these replacements in the following. From the viewpoint of Eve, steps (1) and (1′) are equivalent because the probability that a signal with n_A photons is emitted from Alice is $P_{\mu_A}^{\text{Poisson}}(n_A)$ and the probabilities that its polarization is H, V, D, and $\bar{D}$ are $p_Z/2, p_Z/2, p_X/2$, and $p_X/2$, respectively, in both steps. The replacement from step (1) to step (1′) is called the "source replacement" scheme [22]. In step (2), the outcome of the actual measurement does not change even if Bob first conducts the QND measurement, because the positive operator-valued measure (POVM) elements of the actual measurement are block-diagonalized in terms of the photon number n_B [6]. The common transmittance η_Z between the Z line and the X line in Fig. 1 can be considered to be absorbed by Eve's quantum channel, while the additional transmittance r [defined in Eq. (3)] for the X line is left. The equivalent setup to Fig. 1 is thus shown in Fig. 3. We often see a scenario where the dark counts are regarded as noise in Eve's quantum channel, but that holds only when dark counts do not influence the probability of basis choice. The protocol with active basis choice and the protocol with passive *balanced* basis choice satisfy this condition, while the protocol with passive biased basis choice, which is the target of this paper, does not satisfy the condition. Thus, the dark-count probability d is left in Fig. 3, while the quantum efficiency of detectors can be regarded as 1. Next, we divide the X line into two lines. As shown in Fig. 2, we introduce the X' line corresponding to the path along which light is transmitted by the beam splitter with a transmittance r to reach detectors in Fig. 3. We introduce the L line corresponding to the path along which light is reflected by the beam splitter in Fig. 3, and also introduce the Z' line corresponding to the Z line in Fig. 3. Consequently, in Fig. 2, incoming light is split into three passes, the Z' line, X' line, and L line, with the splitting ratio of $p_{Z'} = p_Z$, $p_{X'} = p_X r$, and $p_L = 1 - p_{Z'} - p_{X'}$, respectively. There is no loss in the Z' line and X' line any more. Thus we obtain step (2′).

In the alternative protocol, photon numbers n_A and n_B are regarded as observed numbers, which enables us to

define the following ratios for $W \in \{Z, X\}$:

$$\begin{aligned} Q^{(n'_A,n'_B)} &:= m(y_B = 1 \wedge n_A = n'_A \wedge n_B = n'_B)/m_{\mathrm{gen}}, \\ Q_W^{(n'_A,n'_B)} &:= m(y_B = 1 \wedge W_A = W_B = W \\ &\quad \wedge n_A = n'_A \wedge n_B = n'_B)/m_{\mathrm{gen}}, \\ E_W^{(n'_A,n'_B)} &:= m(y_B = 1 \wedge W_A = W_B = W \\ &\quad \wedge n_A = n'_A \wedge n_B = n'_B \wedge b_A \neq b_B)/m_{\mathrm{gen}}, \\ Q_{\mathrm{cross}}^{(n'_A,n'_B)} &:= m(y_B = 1 \wedge W_B = \perp \\ &\quad \wedge n_A = n'_A \wedge n_B = n'_B)/m_{\mathrm{gen}}. \end{aligned} \tag{9}$$

In this paper, the security proof with complementarity [8,9] is applied where the "phase error" rate is bounded by observed values in the actual protocol. The phase error is defined as a bit error when Alice virtually measures system A of $|\Phi_Z^{(n_A)}\rangle_{AA'}$ in the X basis instead of the Z basis to obtain a bit value $\tilde{b}_A$, and Bob outputs a bit value $\tilde{b}_B$ as a guess for Alice's measurement outcome $\tilde{b}_A$. By defining

$$\begin{aligned} E_{\mathrm{ph}}^{(n'_A,n'_B)} &:= m(y_B = 1 \wedge W_A = W_B = Z \\ &\quad \wedge n_A = n'_A \wedge n_B = n'_B \wedge \tilde{b}_A \neq \tilde{b}_B)/m_{\mathrm{gen}}, \end{aligned} \tag{10}$$

the phase error rate is represented as $E_{\mathrm{ph}}^{(n_A,n_B)}/Q_Z^{(n_A,n_B)}$. Since the X and Z bases are complementary, the more Bob can estimate Alice's X-basis measurement outcomes, i.e., less phase error rate, the less Alice's Z-basis measurement outcomes (a secret key) are leaked to Eve. That is, a smaller phase error rate implies a smaller amount of privacy amplification.

Now consider the dependency of the phase error rate on photon numbers n_A and n_B. For $n_A \geq 2$, the phase error rate is regarded as 1/2. This is physically achieved when Eve extracts one photon from two photons emitted from Alice, for example, which is called a photon-number splitting attack [26]. For $n_A = 1$ and $n_B \geq 2$, in this paper, we regard the phase error rate as 1/2, i.e., arrivals of multiple photons are assumed to be totally insecure. For $n_A = 1$ and $n_B = 0$, the phase error rate is 1/2 because Bob's measurement outcome purely originates from dark counts and he cannot estimate Alice's X-basis measurement outcome at all. For $n_A = 0$, from Eq. (8), Bob always knows that Alice's X-basis measurement result is 0, and thus the phase error rate is 0. For $n_A = 1$ and $n_B = 1$, the phase error rate is nontrivial and an upper bound is given in the following section. As a consequence, the alternative protocol is secure if the ratio of privacy amplification is

$$\begin{aligned} f_{\mathrm{PA}}^{\mathrm{alt}} = &\sum_{n_A \geq 2, n_B \geq 0} Q_Z^{(n_A,n_B)} + \sum_{n_B \geq 2} Q_Z^{(1,n_B)} + Q_Z^{(1,0)} \\ &+ Q_Z^{(1,1)} h\left(\frac{E_{\mathrm{ph}}^{(1,1)}}{Q_Z^{(1,1)}}\right), \end{aligned} \tag{11}$$

where $h(x) := -x \log_2 x - (1-x)\log_2(1-x)$ represents the binary entropy. However, each term is not observable in the actual protocol, and thus we derive an upper bound on $f_{\mathrm{PA}}^{\mathrm{alt}}$ using observed quantities.

B. Upper bounding on parameters in $f_{\mathrm{PA}}^{\mathrm{alt}}$

In this subsection, we show that an upper bound on $f_{\mathrm{PA}}^{\mathrm{alt}}$ is given by bounds on quantities obtained by the decoy-state method. The bound on $f_{\mathrm{PA}}^{\mathrm{alt}}$ is derived from upper bounds on the phase error rate in rounds with single-photon detection and on the rate of multiple-photon detection.

1. Upper bound on single-photon phase error rate

Here we derive an upper bound on $E_{\mathrm{ph}}^{(1,1)}$. The key idea is to find a protocol with Bob's active basis choice that is equivalent to the alternative protocol. We define B as the system before Bob's passive splitter in Fig. 2, and also define Z', X', and L as systems of the Z' line, X' line, and L line, respectively. Let $\hat{b}_H^\dagger$ and $\hat{b}_V^\dagger$ be the creation operators of horizontal and vertical polarizations, respectively, and $\hat{b}_D^\dagger := (\hat{b}_H^\dagger + \hat{b}_V^\dagger)/\sqrt{2}$ and $\hat{b}_{\bar{D}}^\dagger := (\hat{b}_H^\dagger - \hat{b}_V^\dagger)/\sqrt{2}$ be operators of diagonal polarizations in system B. Similarly, define $(\hat{z}_H^\dagger, \hat{z}_V^\dagger)$, $(\hat{x}_H^\dagger, \hat{x}_V^\dagger)$, and $(\hat{l}_H^\dagger, \hat{l}_V^\dagger)$ as sets of creation operators of horizontal and vertical polarizations in systems Z', X', and L, respectively. We also define $\hat{x}_D^\dagger := (\hat{x}_H^\dagger + \hat{x}_V^\dagger)/\sqrt{2}$ and $\hat{x}_{\bar{D}}^\dagger := (\hat{x}_H^\dagger - \hat{x}_V^\dagger)/\sqrt{2}$. With the notation

$$\hat{N}_\xi^{(1)} := \hat{\xi}^\dagger |\mathrm{vac}\rangle \langle \mathrm{vac}|_{Z'X'L} \hat{\xi}, \tag{12}$$

for $\xi \in \{z_H, z_V, x_D, x_{\bar{D}}, l_H, l_V\}$, the POVM elements in system $Z'X'L$ under the condition that the outcome of QND measurement is $n_B = 1$ are described as follows:

$$\begin{aligned} \hat{F}_{Z0}^{(1)} &= [\hat{N}_{z_H}^{(1)} + d(\hat{N}_{l_H}^{(1)} + \hat{N}_{l_V}^{(1)})](1-d)^3, \\ \hat{F}_{Z1}^{(1)} &= [\hat{N}_{z_V}^{(1)} + d(\hat{N}_{l_H}^{(1)} + \hat{N}_{l_V}^{(1)})](1-d)^3, \\ \hat{F}_{Z,\mathrm{double}}^{(1)} &= [d(\hat{N}_{z_H}^{(1)} + \hat{N}_{z_V}^{(1)}) + d^2(\hat{N}_{l_H}^{(1)} + \hat{N}_{l_V}^{(1)})](1-d)^2, \\ \hat{F}_{X0}^{(1)} &= [\hat{N}_{x_D}^{(1)} + d(\hat{N}_{l_H}^{(1)} + \hat{N}_{l_V}^{(1)})](1-d)^3, \end{aligned}$$

$$\begin{aligned}
\hat{F}^{(1)}_{X1} &= [\hat{N}^{(1)}_{x_{\bar{D}}} + d(\hat{N}^{(1)}_{l_H} + \hat{N}^{(1)}_{l_V})](1-d)^3,\\
\hat{F}^{(1)}_{X,\text{double}} &= [d(\hat{N}^{(1)}_{x_D} + \hat{N}^{(1)}_{x_{\bar{D}}}) + d^2(\hat{N}^{(1)}_{l_H} + \hat{N}^{(1)}_{l_V})](1-d)^2,\\
\hat{F}^{(1)}_{\text{no-click}} &= (1-d)^4(\hat{N}^{(1)}_{l_H} + \hat{N}^{(1)}_{l_V}),\\
\hat{F}^{(1)}_{\text{cross}} &= [1-(1-d)^2](\hat{N}^{(1)}_{z_H} + \hat{N}^{(1)}_{z_V} + \hat{N}^{(1)}_{x_D} + \hat{N}^{(1)}_{x_{\bar{D}}})\\
&\quad + [1-(1-d)^2]^2(\hat{N}^{(1)}_{l_H} + \hat{N}^{(1)}_{l_V}),
\end{aligned} \tag{13}$$

with $\hat{F}^{(1)}_{W'b}$ corresponding to the outcome $b \in \{0,1\}$ in the $W' \in \{Z', X'\}$ line, $\hat{F}^{(1)}_{W',\text{double}}$ corresponding to the double-click events in the $W' \in \{Z', X'\}$ line, $\hat{F}^{(1)}_{\text{no-click}}$ corresponding to the no-detection event, and $\hat{F}^{(1)}_{\text{cross}}$ corresponding to cross-click events. Note that the sum of the above POVM elements equals the projection onto the single-photon subspace of the $Z'X'L$ system:

$$\hat{\mathbb{1}}^{(1)}_{Z'X'L} := \hat{N}^{(1)}_{z_H} + \hat{N}^{(1)}_{z_V} + \hat{N}^{(1)}_{x_D} + \hat{N}^{(1)}_{x_{\bar{D}}} + \hat{N}^{(1)}_{l_H} + \hat{N}^{(1)}_{l_V}. \tag{14}$$

Now we rewrite those POVM elements as operators on system B instead of system $Z'X'L$. An ancillary system EE' is introduced so that the dimension of BEE' equals that of $Z'X'L$. Let $\hat{U}$ be a unitary operator from BEE' to $Z'X'L$ representing evolution of the passive splitter in Fig. 2, whose action is

$$\begin{aligned}
\hat{U}\hat{b}^\dagger_H\hat{U}^\dagger &= \sqrt{p_{Z'}}\,\hat{z}^\dagger_H + \sqrt{p_{X'}}\,\hat{x}^\dagger_H + \sqrt{p_L}\,\hat{l}^\dagger_H,\\
\hat{U}\hat{b}^\dagger_V\hat{U}^\dagger &= \sqrt{p_{Z'}}\,\hat{z}^\dagger_V + \sqrt{p_{X'}}\,\hat{x}^\dagger_V + \sqrt{p_L}\,\hat{l}^\dagger_V.
\end{aligned} \tag{15}$$

Here we define a projection operator $\hat{M}^{(1)}_{B,H}$ from the single-photon subspace on system B onto $\hat{z}^\dagger_H|\text{vac}\rangle_{Z'X'L}$, which is described as $\hat{M}^{(1)}_{B,H} = {}_{Z'X'L}\langle\text{vac}|\,\hat{z}_H\hat{U}\,|\text{vac}\rangle_{EE'}$. Let us also define

$$\begin{aligned}
|H\rangle_B &:= \hat{b}^\dagger_H|\text{vac}\rangle_B, \quad |V\rangle_B := \hat{b}^\dagger_V|\text{vac}\rangle_B,\\
|D\rangle_B &:= \hat{b}^\dagger_D|\text{vac}\rangle_B, \quad |\bar{D}\rangle_B := \hat{b}^\dagger_{\bar{D}}|\text{vac}\rangle_B.
\end{aligned} \tag{16}$$

By denoting $\hat{M}^{(1)}_{B,H}|H\rangle_B =: \gamma_{HH}$ and $\hat{M}^{(1)}_{B,H}|V\rangle_B =: \gamma_{HV}$,

$$\hat{M}^{(1)}_{B,H} = \hat{M}^{(1)}_{B,H}\hat{\mathbb{1}}^{(1)}_B = {}_B\langle H|\,\gamma_{HH} + {}_B\langle V|\,\gamma_{HV} \tag{17}$$

holds, where we have defined $\hat{\mathbb{1}}^{(1)}_B := |H\rangle\langle H|_B + |V\rangle\langle V|_B$. Now we calculate γ_{HH} and γ_{HV} as follows:

$$\begin{aligned}
\gamma_{HH} &= {}_{Z'X'L}\langle\text{vac}|\,\hat{z}_H\hat{U}\hat{b}^\dagger_H\,|\text{vac}\rangle_{BEE'}\\
&= {}_{Z'X'L}\langle\text{vac}|\,\hat{z}_H\hat{U}\hat{b}^\dagger_H\hat{U}^\dagger\,|\text{vac}\rangle_{Z'X'L}\\
&= {}_{Z'X'L}\langle\text{vac}|\,\hat{z}_H(\sqrt{p_{Z'}}\,\hat{z}^\dagger_H + \sqrt{p_{X'}}\,\hat{x}^\dagger_H\\
&\quad + \sqrt{p_L}\,\hat{l}^\dagger_H)\,|\text{vac}\rangle_{Z'X'L}\\
&= \sqrt{p_{Z'}},\\
\gamma_{HV} &= {}_{Z'X'L}\langle\text{vac}|\,\hat{z}_H(\sqrt{p_{Z'}}\,\hat{z}^\dagger_V + \sqrt{p_{X'}}\,\hat{x}^\dagger_V\\
&\quad + \sqrt{p_L}\,\hat{l}^\dagger_V)\,|\text{vac}\rangle_{Z'X'L}\\
&= 0.
\end{aligned} \tag{18}$$

Therefore, from Eq. (17), we obtain $\hat{M}^{(1)}_{B,H} = {}_B\langle H|\sqrt{p_{Z'}}$, and thus the POVM element on system B is $\hat{M}^{(1)\dagger}_{B,H}\hat{M}^{(1)}_{B,H} = p_{Z'}|H\rangle\langle H|_B$. Similarly, we have the following relations:

$$\begin{aligned}
&\hat{N}^{(1)}_{z_H} \to p_{Z'}|H\rangle\langle H|_B, \quad \hat{N}^{(1)}_{z_V} \to p_{Z'}|V\rangle\langle V|_B,\\
&\hat{N}^{(1)}_{x_D} \to p_{X'}|D\rangle\langle D|_B, \quad \hat{N}^{(1)}_{x_{\bar{D}}} \to p_{X'}|\bar{D}\rangle\langle\bar{D}|_B,\\
&\hat{N}^{(1)}_{l_H} \to p_L|H\rangle\langle H|_B, \quad \hat{N}^{(1)}_{l_V} \to p_L|V\rangle\langle V|_B.
\end{aligned} \tag{19}$$

From these results, the POVM elements in Eq. (13) are represented with operators on system B as follows:

$$\begin{aligned}
\hat{F}'^{(1)}_{Z0} &= (p_{Z'}|H\rangle\langle H|_B + p_L d\hat{\mathbb{1}}^{(1)}_B)(1-d)^3,\\
\hat{F}'^{(1)}_{Z1} &= (p_{Z'}|V\rangle\langle V|_B + p_L d\hat{\mathbb{1}}^{(1)}_B)(1-d)^3,\\
\hat{F}'^{(1)}_{Z,\text{double}} &= (p_{Z'}d + p_L d^2)(1-d)^2\hat{\mathbb{1}}^{(1)}_B,\\
\hat{F}'^{(1)}_{X0} &= (p_{X'}|D\rangle\langle D|_B + p_L d\hat{\mathbb{1}}^{(1)}_B)(1-d)^3,\\
\hat{F}'^{(1)}_{X1} &= (p_{X'}|\bar{D}\rangle\langle\bar{D}|_B + p_L d\hat{\mathbb{1}}^{(1)}_B)(1-d)^3,\\
\hat{F}'^{(1)}_{X,\text{double}} &= (p_{X'}d + p_L d^2)(1-d)^2\hat{\mathbb{1}}^{(1)}_B,\\
\hat{F}'^{(1)}_{\text{no-click}} &= p_L(1-d)^4\hat{\mathbb{1}}^{(1)}_B,\\
\hat{F}'^{(1)}_{\text{cross}} &= [1-(1+2p_L d - p_L d^2)(1-d)^2]\hat{\mathbb{1}}^{(1)}_B.
\end{aligned} \tag{20}$$

Note that the sum of those elements equals $\hat{\mathbb{1}}^{(1)}_B$. Including classical postprocessing, the outcomes are limited to "0," "1," and "failure," where "failure" corresponds to the no-detection or cross-click round. Since a random bit is assigned to a double-click round, POVM elements

including the postprocessing are as follows:

$$\begin{aligned}
&\hat{G}^{(1)}_{Z0} = \hat{F}'^{(1)}_{Z0} + \tfrac{1}{2}\hat{F}'^{(1)}_{Z,\mathrm{double}}, \quad \hat{G}^{(1)}_{Z1} = \hat{F}'^{(1)}_{Z1} + \tfrac{1}{2}\hat{F}'^{(1)}_{Z,\mathrm{double}},\\
&\hat{G}^{(1)}_{X0} = \hat{F}'^{(1)}_{X0} + \tfrac{1}{2}\hat{F}'^{(1)}_{X,\mathrm{double}}, \quad \hat{G}^{(1)}_{X1} = \hat{F}'^{(1)}_{X1} + \tfrac{1}{2}\hat{F}'^{(1)}_{X,\mathrm{double}},\\
&\hat{G}^{(1)}_{\mathrm{fail}} = \hat{F}'^{(1)}_{\text{no-click}} + \hat{F}'^{(1)}_{\mathrm{cross}}.
\end{aligned} \tag{21}$$

Furthermore, since

$$\begin{aligned}
\hat{G}^{(1)}_{Z0} + \hat{G}^{(1)}_{Z1} &= (p_{Z'} + 2p_L d - p_L d^2)(1-d)^2 \hat{\mathbb{1}}^{(1)}_B,\\
\hat{G}^{(1)}_{X0} + \hat{G}^{(1)}_{X1} &= (p_{X'} + 2p_L d - p_L d^2)(1-d)^2 \hat{\mathbb{1}}^{(1)}_B
\end{aligned} \tag{22}$$

hold, the probabilities that the Z-basis and X-basis measurements are conducted at Bob's site in a round with $n_B = 1$ are $s_Z := (p_{Z'} + 2p_L d - p_L d^2)(1-d)^2$ and $s_X := (p_{X'} + 2p_L d - p_L d^2)(1-d)^2$, respectively, independently of the state given by Eve. Therefore, the measurement with POVM elements in Eq. (21) are realized by the protocol where Bob filters an incoming signal with the success probability $s_Z + s_X$ and *actively* chooses the Z (X) basis with probability

$$\tilde{p}_Z := \frac{s_Z}{s_Z + s_X}, \quad \tilde{p}_X := \frac{s_X}{s_Z + s_X}, \tag{23}$$

respectively, followed by the measurement $\{\hat{G}^{(1)}_{Z0}/s_Z, \hat{G}^{(1)}_{Z1}/s_Z\}$ for the Z basis and $\{\hat{G}^{(1)}_{X0}/s_X, \hat{G}^{(1)}_{X1}/s_X\}$ for the X basis to deterministically obtain the outcome "0" or "1." Here we note that $s_Z \geq s_X$ holds from $p_{Z'} \geq p_{X'}$, which leads to

$$\tilde{p}_Z \geq \tilde{p}_X. \tag{24}$$

In this active protocol, Bob is allowed to perform X-basis measurement after the successful filtering even if he chooses $W_B = Z$, and then Bob's guess $\tilde{b}_B$ in the definition of $E^{(1,1)}_{\mathrm{ph}}$ in Eq. (10) is defined as the output of this X-basis measurement. Notice that this measurement on the filtered state is equivalent to the X-basis measurement performed under the choice of $W_B = X$. On the other hand, in a round with $n_A = 1$, from Eq. (7), Alice sends system A' in state $|\Phi^{(1)}_Z\rangle_{AA'}$ to Bob independently of her basis choice and anyway performs X-basis measurement to estimate $E^{(1,1)}_X$ for the choice of $W_A = X$ and $E^{(1,1)}_{\mathrm{ph}}$ for the choice of $W_A = Z$. Hence, by considering that Alice chooses the Z (X) basis with probability p_Z (p_X) and Bob chooses the Z (X) basis with probability $\tilde{p}_Z$ ($\tilde{p}_X$), we have

$$E^{(1,1)}_{\mathrm{ph}} \sim \frac{p_Z \tilde{p}_Z}{p_X \tilde{p}_X} E^{(1,1)}_X \tag{25}$$

in the asymptotic limit of $m_{\mathrm{rep}} \to \infty$. Here "$\sim$" denotes asymptotic equivalence.

Next we derive an upper bound on $E^{(1,1)}_{\mathrm{ph}}$ with Eq. (25). By defining a quantity that can be estimated with the decoy-state method as

$$E^{(n_A=1)}_X := \sum_{n_B \geq 0} E^{(1,n_B)}_X, \tag{26}$$

we obtain

$$E^{(1,1)}_X = E^{(n_A=1)}_X - E^{(1,0)}_X - \sum_{n_B \geq 2} E^{(1,n_B)}_X \leq E^{(n_A=1)}_X - E^{(1,0)}_X. \tag{27}$$

Since a bit in a round with $n_B = 0$ originates from dark counts of detectors and the dark count rates are the same between both detectors in the X' line, the bit error occurs with the probability 1/2, which leads to

$$E^{(1,0)}_X \sim \tfrac{1}{2} Q^{(1,0)}_X \tag{28}$$

in the asymptotic limit. On the other hand,

$$Q^{(1,0)}_X \sim \frac{p_X}{p_Z} Q^{(1,0)}_Z \tag{29}$$

holds in the asymptotic limit because Alice can be deemed to choose her basis independently at the end for the choice of $n_A = 1$ from Eq. (7), while all detectors in the Z' line and the X' line have the same dark count rate. From Eqs. (25) and (27)–(29), we have

$$\begin{aligned}
E^{(1,1)}_{\mathrm{ph}} &\lesssim \frac{p_Z \tilde{p}_Z}{p_X \tilde{p}_X} \left(E^{(n_A=1)}_X - \frac{1}{2}\frac{p_X}{p_Z} Q^{(1,0)}_Z \right)\\
&= \frac{p_Z \tilde{p}_Z}{p_X \tilde{p}_X} E^{(n_A=1)}_X - \frac{1}{2}\frac{\tilde{p}_Z}{\tilde{p}_X} Q^{(1,0)}_Z,
\end{aligned} \tag{30}$$

where "$\lesssim$" is used for an inequality that holds in the asymptotic limit.

Here we derive an upper bound on the quantity $f^{\mathrm{alt}}_{\mathrm{PA}}$ of privacy amplification in Eq. (11) by using Eq. (30). Let us define

$$Q^{(n_A=1)}_Z := \sum_{n_B \geq 0} Q^{(1,n_B)}_Z, \tag{31}$$

which can be estimated with the decoy-state method, and define $q_Z := Q^{(n_A=1)}_Z - \sum_{n_B \geq 2} Q^{(1,n_B)}_Z$ (≥ 0). Since $Q^{(1,1)}_Z = q_Z - Q^{(1,0)}_Z$ holds, we have

$$\begin{aligned}\frac{Q_Z^{(1,0)}+Q_Z^{(1,1)}h(E_{\rm ph}^{(1,1)}/Q_Z^{(1,1)})}{q_Z} &= \frac{Q_Z^{(1,0)}}{q_Z}h\left(\frac{1}{2}\right)+\frac{q_Z-Q_Z^{(1,0)}}{q_Z}h\left(\frac{E_{\rm ph}^{(1,1)}}{q_Z-Q_Z^{(1,0)}}\right)\le h\left(\frac{Q_Z^{(1,0)}}{2q_Z}+\frac{E_{\rm ph}^{(1,1)}}{q_Z}\right)\\ &\lesssim h\left(\frac{Q_Z^{(1,0)}}{2q_Z}+\frac{p_Z\tilde{p}_Z}{q_Z p_X\tilde{p}_X}E_X^{(n_A=1)}-\frac{Q_Z^{(1,0)}}{2q_Z}\frac{\tilde{p}_Z}{\tilde{p}_X}\right)\\ &= h\left(\frac{Q_Z^{(1,0)}}{2q_Z}\left(1-\frac{\tilde{p}_Z}{\tilde{p}_X}\right)+\frac{p_Z\tilde{p}_Z}{q_Z p_X\tilde{p}_X}E_X^{(n_A=1)}\right)\\ &\le h\left(\frac{p_Z\tilde{p}_Z}{q_Z p_X\tilde{p}_X}E_X^{(n_A=1)}\right).\end{aligned} \tag{32}$$

Here the first inequality uses concavity of the binary entropy, the second inequality uses Eq. (30), and the third inequality uses $\tilde{p}_Z/\tilde{p}_X \ge 1$ from Eq. (24). In addition, the second and third inequalities also use the property of the binary entropy $h(x)$ such that it is a monotonically increasing function with x in the range $0 \le x \le 1/2$. To use this property, the sufficient condition is

$$\frac{p_Z\tilde{p}_Z}{p_X\tilde{p}_X}E_X^{(n_A=1)} \lesssim \frac{q_Z}{2} \tag{33}$$

and we derive the condition for observed parameters in the actual protocol to satisfy Eq. (33) in Sec. III D.

Let us define

$$Q_Z^{(n_A=0)} := \sum_{n_B\ge 0} Q_Z^{(0,n_B)}, \tag{34}$$

which can be estimated with the decoy-state method. The quantity $f_{\rm PA}^{\rm alt}$ of privacy amplification in Eq. (11) is upper-bounded as follows:

$$\begin{aligned}f_{\rm PA}^{\rm alt} &= \sum_{n_A\ge 2,\, n_B\ge 0} Q_Z^{(n_A,n_B)}+\sum_{n_B\ge 2}Q_Z^{(1,n_B)}+Q_Z^{(1,0)}+Q_Z^{(1,1)}h\left(\frac{E_{\rm ph}^{(1,1)}}{Q_Z^{(1,1)}}\right)\\ &\lesssim \sum_{n_A\ge 2,\, n_B\ge 0} Q_Z^{(n_A,n_B)}+\sum_{n_B\ge 2}Q_Z^{(1,n_B)}+q_Z h\left(\frac{p_Z\tilde{p}_Z}{q_Z p_X\tilde{p}_X}E_X^{(n_A=1)}\right)\\ &= Q_Z-Q_Z^{(n_A=0)}-Q_Z^{(n_A=1)}+\sum_{n_B\ge 2}Q_Z^{(1,n_B)}+q_Z h\left(\frac{p_Z\tilde{p}_Z}{q_Z p_X\tilde{p}_X}E_X^{(n_A=1)}\right)\\ &= Q_Z-Q_Z^{(n_A=0)}-q_Z\left(1-h\left(\frac{p_Z\tilde{p}_Z}{q_Z p_X\tilde{p}_X}E_X^{(n_A=1)}\right)\right)\\ &= Q_Z-Q_Z^{(n_A=0)}-\left(Q_Z^{(n_A=1)}-\sum_{n_B\ge 2}Q_Z^{(1,n_B)}\right)\left(1-h\left(\frac{p_Z\tilde{p}_Z E_X^{(n_A=1)}}{p_X\tilde{p}_X(Q_Z^{(n_A=1)}-\sum_{n_B\ge 2}Q_Z^{(1,n_B)})}\right)\right).\end{aligned} \tag{35}$$

This inequality implies that an upper bound on $\sum_{n_B\ge 2}Q_Z^{(1,n_B)}$ gives a further upper bound on $f_{\rm PA}^{\rm alt}$.

2. Upper bound on multiple-photon contribution

Here we derive an upper bound on $\sum_{n_B\ge 2}Q_Z^{(1,n_B)}$ in Eq. (35) by considering cases with given n_B (≥ 2). The key idea is to estimate the contribution of multiple photons to key generation by using the number of cross-click events that are observed uniquely in the passive protocol [21]. Let us define the following Fock states on system B and system $Z'X'L$:

$$|\vec{m}_B\rangle_B = |m_H,m_V\rangle_B := \frac{(\hat{b}_H^\dagger)^{m_H}(\hat{b}_V^\dagger)^{m_V}}{\sqrt{m_H!\,m_V!}}|{\rm vac}\rangle_B \tag{36}$$

and

$$
\begin{aligned}
&|\vec{m}_{Z'X'L}\rangle_{Z'X'L} \\
&\quad = |m_{ZH}, m_{ZV}, m_{XH}, m_{XV}, m_{LH}, m_{LV}\rangle_{Z'X'L} \\
&\quad := \frac{(\hat{z}_H^\dagger)^{m_{ZH}}(\hat{z}_V^\dagger)^{m_{ZV}}(\hat{x}_H^\dagger)^{m_{XH}}(\hat{x}_V^\dagger)^{m_{XV}}(\hat{l}_H^\dagger)^{m_{LH}}(\hat{l}_V^\dagger)^{m_{LV}}}{\sqrt{m_{ZH}!\, m_{ZV}!\, m_{XH}!\, m_{XV}!\, m_{LH}!\, m_{LV}!}} \\
&\qquad \times |\mathrm{vac}\rangle_{Z'X'L}\,. \qquad (37)
\end{aligned}
$$

We denote the following four POVM elements on system $Z'X'L$: elements $\hat{F}_W^{(n_B)}$ corresponding to key generation in the $W \in \{Z, X\}$ basis; an element $\hat{F}_{\text{no-click}}^{(n_B)}$ corresponding to the no-detection event; and an element $\hat{F}_{\text{cross}}^{(n_B)}$ corresponding to cross-click events. By using the basis states in Eq. (37) with the notation $P(|\cdot\rangle) := |\cdot\rangle\langle\cdot|$, the element $\hat{F}_Z^{(n_B)}$ is described as

$$
\begin{aligned}
\hat{F}_Z^{(n_B)} = (1-d)^2 \Bigg(&\sum_{m_H=0}^{n_B} \sum_{m_{ZH}=0}^{m_H} \sum_{m_{ZV}=0}^{n_B-m_H} P(|m_{ZH}, m_{ZV}, 0, 0, m_H - m_{ZH}, n_B - m_H - m_{ZV}\rangle_{Z'X'L}) \\
&- \sum_{m_H=0}^{n_B} (1-d)^2 P(|0,0,0,0,m_H, n_B - m_H\rangle_{Z'X'L}) \Bigg), \qquad (38)
\end{aligned}
$$

where the second term in Eq. (38) corresponds to an event where all photons go to the L line and no dark count occurs in the Z' line. Similarly, the other elements are described as follows:

$$
\begin{aligned}
\hat{F}_X^{(n_B)} = (1-d)^2 \Bigg(&\sum_{m_H=0}^{n_B} \sum_{m_{XH}=0}^{m_H} \sum_{m_{XV}=0}^{n_B-m_H} P(|0, 0, m_{XH}, m_{XV}, m_H - m_{XH}, n_B - m_H - m_{XV}\rangle_{Z'X'L}) \\
&- \sum_{m_H=0}^{n_B} (1-d)^2 P(|0,0,0,0,m_H, n_B - m_H\rangle_{Z'X'L}) \Bigg), \qquad (39)
\end{aligned}
$$

$$
\hat{F}_{\text{no-click}}^{(n_B)} = (1-d)^4 \sum_{m_H=0}^{n_B} P(|0,0,0,0,m_H, n_B - m_H\rangle_{Z'X'L}), \qquad (40)
$$

$$
\hat{F}_{\text{cross}}^{(n_B)} = \hat{\mathbb{1}}_{Z'X'L}^{(n_B)} - \hat{F}_Z^{(n_B)} - \hat{F}_X^{(n_B)} - \hat{F}_{\text{no-click}}^{(n_B)}, \qquad (41)
$$

where

$$
\hat{\mathbb{1}}_{Z'X'L}^{(n_B)} := \sum_{\substack{\vec{m}_{Z'X'L} \in \{\vec{m}_{Z'X'L} \,|\, m_{ZH}+m_{ZV} \\ +m_{XH}+m_{XV}+m_{LH}+m_{LV}=n_B\}}} P(|\vec{m}_{Z'X'L}\rangle_{Z'X'L}). \qquad (42)
$$

Again we introduce an ancillary system EE' so that the dimension of BEE' equals that of the system $Z'X'L$. Let $\hat{\mathbb{1}}_{BEE'}^{(n_B)}$ be an identity operator in the n_B-photon subspace on system BEE'. Using the unitary operator $\hat{U}$ indicating evolution given by the passive splitter,

$$
\hat{\mathbb{1}}_{BEE'}^{(n_B)} = \hat{U}^\dagger \hat{\mathbb{1}}_{Z'X'L}^{(n_B)} \hat{U} \qquad (43)
$$

holds. Here we define

$$
\hat{\mathbb{1}}_B^{(n_B)} := \sum_{\vec{m}_B \in \{\vec{m}_B \,|\, m_H + m_V = n_B\}} P(|\vec{m}_B\rangle_B), \qquad (44)
$$

and we then have

$$
{}_{EE'}\langle \mathrm{vac}|\, \hat{U}^\dagger \hat{\mathbb{1}}_{Z'X'L}^{(n_B)} \hat{U} |\mathrm{vac}\rangle_{EE'} = \hat{\mathbb{1}}_B^{(n_B)}. \qquad (45)
$$

Now we represent $\hat{F}_Z^{(n_B)}$ in Eq. (38) in terms of system B. Let us define

$$|\vec{m}_{Z'L}\rangle_{Z'X'L} := |m_{ZH}, m_{ZV}, 0, 0, m_H - m_{ZH}, n_B - m_H - m_{ZV}\rangle_{Z'X'L}. \tag{46}$$

A measurement operator $\hat{M}_{\vec{m}_{Z'L}} : B \to \mathbb{C}$ that corresponds to the projection onto $|\vec{m}_{Z'L}\rangle_{Z'X'L}$ is represented as $\hat{M}_{\vec{m}_{Z'L}} = {}_{Z'X'L}\langle\vec{m}_{Z'L}|\,\hat{U}\,|\mathrm{vac}\rangle_{EE'}$. For arbitrary

$$|\vec{m}'_B\rangle_B := |m'_H, m'_V\rangle_B, \tag{47}$$

let $\gamma_{\vec{m}'_B,\vec{m}_{Z'L}} := \hat{M}_{\vec{m}_{Z'L}}\,|\vec{m}'_B\rangle_B$. Then we can write $\hat{M}_{\vec{m}_{Z'L}}$ as

$$\hat{M}_{\vec{m}_{Z'L}} = \hat{M}_{\vec{m}_{Z'L}} \sum_{\vec{m}'_B} |\vec{m}'_B\rangle\,\langle\vec{m}'_B|_B = \sum_{\vec{m}'_B} {}_B\langle\vec{m}'_B|\,\gamma_{\vec{m}'_B,\vec{m}_{Z'L}}. \tag{48}$$

By using Eq. (15), we calculate $\gamma_{\vec{m}'_B,\vec{m}_{Z'L}}$ as follows:

$$\begin{aligned}
\gamma_{\vec{m}'_B,\vec{m}_{Z'L}} &= {}_{Z'X'L}\langle\vec{m}_{Z'L}|\hat{U}|\vec{m}'\rangle_B\,|\mathrm{vac}\rangle_{EE'} \\
&= {}_{Z'X'L}\langle\vec{m}_{Z'L}|\frac{\hat{U}(\hat{b}_H^\dagger)^{m'_H}(\hat{b}_V^\dagger)^{m'_V}}{\sqrt{m'_H!\,m'_V!}}|\mathrm{vac}\rangle_{BEE'} \\
&= {}_{Z'X'L}\langle\vec{m}_{Z'L}|\frac{(\hat{U}\hat{b}_H^\dagger\hat{U}^\dagger)^{m'_H}(\hat{U}\hat{b}_V^\dagger\hat{U}^\dagger)^{m'_V}}{\sqrt{m'_H!\,m'_V!}}|\mathrm{vac}\rangle_{Z'X'L} \\
&= {}_{Z'X'L}\langle\vec{m}_{Z'L}|\frac{1}{\sqrt{m'_H!\,m'_V!}}\left(\sqrt{p_{Z'}}\,\hat{z}_H^\dagger + \sqrt{p_{X'}}\,\hat{x}_H^\dagger + \sqrt{p_L}\,\hat{l}_H^\dagger\right)^{m'_H}\left(\sqrt{p_{Z'}}\,\hat{z}_V^\dagger + \sqrt{p_{X'}}\,\hat{x}_V^\dagger + \sqrt{p_L}\,\hat{l}_V^\dagger\right)^{m'_V}|\mathrm{vac}\rangle_{Z'X'L} \\
&= {}_{Z'X'L}\langle\vec{m}_{Z'L}|\frac{1}{\sqrt{m'_H!\,m'_V!}}\sum_{(i,j)\in S_{m'_H}}\frac{m'_H!}{i!j!(m'_H-i-j)!}(\sqrt{p_{Z'}}\,\hat{z}_H^\dagger)^i(\sqrt{p_{X'}}\,\hat{x}_H^\dagger)^j(\sqrt{p_L}\,\hat{l}_H^\dagger)^{m'_H-i-j} \\
&\quad\times\sum_{(i',j')\in S_{m'_V}}\frac{m'_V!}{i'!j'!(m'_V-i'-j')!}(\sqrt{p_{Z'}}\,\hat{z}_V^\dagger)^{i'}(\sqrt{p_{X'}}\,\hat{x}_V^\dagger)^{j'}(\sqrt{p_L}\,\hat{l}_V^\dagger)^{m'_V-i'-j'}|\mathrm{vac}\rangle_{Z'X'L} \\
&= {}_{Z'X'L}\langle\vec{m}_{Z'L}|\sum_{(i,j)\in S_{m'_H}}\sum_{(i',j')\in S_{m'_V}}\sqrt{\frac{m'_H!}{i!j!(m'_H-i-j)!}\frac{m'_V!}{i'!j'!(m'_V-i'-j')!}}\,(\sqrt{p_{Z'}})^{i+i'}(\sqrt{p_{X'}})^{j+j'} \\
&\quad\times(\sqrt{p_L})^{m'_H+m'_V-i-j-i'-j'}|i,i',j,j',m'_H-i-j,m'_V-i'-j'\rangle_{Z'X'L},
\end{aligned} \tag{49}$$

where $S_{m'_H} = \{(i,j)\mid i+j \le m'_H\}$ and $S_{m'_V} = \{(i',j')\mid i'+j' \le m'_V\}$. From Eq. (46), a term in Eq. (49) is not zero only if $i = m_{ZH}$, $i' = m_{ZV}$, $j = 0$, $j' = 0$, $m'_H = m_H$, and $m'_V = n_B - m_H$ hold. If $m'_H \neq m_H$ or $m'_V \neq n_B - m_H$, then $\gamma_{\vec{m}'_B,\vec{m}_{Z'L}} = 0$, and if $m'_H = m_H$ and $m'_V = n_B - m_H$, then

$$\begin{aligned}
\gamma_{\vec{m}'_B,\vec{m}_{Z'L}} &= \sqrt{\frac{m_H!}{m_{ZH}!(m_H-m_{ZH})!}\frac{(n_B-m_H)!}{m_{ZV}!(n_B-m_H-m_{ZV})!}}\,(\sqrt{p_{Z'}})^{m_{ZH}+m_{ZV}}(\sqrt{p_L})^{n_B-m_{ZH}-m_{ZV}} \\
&= \sqrt{\binom{m_H}{m_{ZH}}\binom{n_B-m_H}{m_{ZV}}}\,(\sqrt{p_{Z'}})^{m_{ZH}+m_{ZV}}(\sqrt{p_L})^{n_B-m_{ZH}-m_{ZV}}.
\end{aligned} \tag{50}$$

From Eq. (48), we obtain

$$\hat{M}_{\vec{m}_{Z'L}} = \sqrt{\binom{m_H}{m_{ZH}}\binom{n_B-m_H}{m_{ZV}}}(\sqrt{p_{Z'}})^{m_{ZH}+m_{ZV}} \times (\sqrt{p_L})^{n_B-m_{ZH}-m_{ZV}}{}_B\langle m_H, n_B-m_H|\,. \quad (51)$$

Thus, a POVM element on system B corresponding to projection onto $|\vec{m}_{Z'L}\rangle_{Z'X'L}$ is

$$\begin{aligned} &P({}_{EE'}\langle \mathrm{vac}|\,\hat{U}^\dagger\,|\vec{m}_{Z'L}\rangle_{Z'X'L}) \\ &= \hat{M}^\dagger_{\vec{m}_{Z'L}}\hat{M}_{\vec{m}_{Z'L}} \\ &= \binom{m_H}{m_{ZH}}\binom{n_B-m_H}{m_{ZV}} p_{Z'}^{m_{ZH}+m_{ZV}} \\ &\quad \times p_L^{n_B-m_{ZH}-m_{ZV}} P(|m_H, n_B-m_H\rangle_B). \end{aligned} \quad (52)$$

By using Eq. (52), the POVM element in Eq. (38) is described in terms of system B as follows:

$$\begin{aligned} \hat{F}'^{(n_B)}_Z &:= {}_{EE'}\langle \mathrm{vac}|\,\hat{U}^\dagger \hat{F}^{(n_B)}_Z \hat{U}\,|\mathrm{vac}\rangle_{EE'} \\ &= (1-d)^2\Bigg(\sum_{m_H=0}^{n_B}\sum_{m_{ZH}=0}^{m_H}\sum_{m_{ZV}=0}^{n_B-m_H}\binom{m_H}{m_{ZH}}\binom{n_B-m_H}{m_{ZV}} \\ &\quad \times p_{Z'}^{m_{ZH}+m_{ZV}} p_L^{n_B-m_{ZH}-m_{ZV}} P(|m_H, n_B-m_H\rangle_B) \\ &\quad - \sum_{m_H=0}^{n_B}(1-d)^2 p_L^{n_B} P(|m_H, n_B-m_H\rangle_B)\Bigg) \\ &= (1-d)^2\Bigg(\sum_{m_H=0}^{n_B}\sum_{m_{ZH}=0}^{m_H}\binom{m_H}{m_{ZH}} p_{Z'}^{m_{ZH}} p_L^{m_H-m_{ZH}} \\ &\quad \times \sum_{m_{ZV}=0}^{n_B-m_H}\binom{n_B-m_H}{m_{ZV}} p_{Z'}^{m_{ZV}} p_L^{n_B-m_H-m_{ZV}} \\ &\quad \times P(|m_H, n_B-m_H\rangle_B) - (1-d)^2 p_L^{n_B}\hat{\mathbb{1}}^{(n_B)}_B\Bigg) \\ &= (1-d)^2\Bigg(\sum_{m_H=0}^{n_B}(p_{Z'}+p_L)^{m_H}(p_{Z'}+p_L)^{n_B-m_H} \\ &\quad \times P(|m_H, n_B-m_H\rangle_B) - (1-d)^2 p_L^{n_B}\hat{\mathbb{1}}^{(n_B)}_B\Bigg) \\ &= (1-d)^2[(p_{Z'}+p_L)^{n_B} - (1-d)^2 p_L^{n_B}]\hat{\mathbb{1}}^{(n_B)}_B. \end{aligned} \quad (53)$$

In similar ways, Eqs. (39) and (40) are described in terms of system B:

$$\begin{aligned} \hat{F}'^{(n_B)}_X &:= {}_{EE'}\langle \mathrm{vac}|\,\hat{U}^\dagger \hat{F}^{(n_B)}_X \hat{U}\,|\mathrm{vac}\rangle_{EE'} \\ &= (1-d)^2[(p_{X'}+p_L)^{n_B} - (1-d)^2 p_L^{n_B}]\hat{\mathbb{1}}^{(n_B)}_B, \end{aligned} \quad (54)$$

$$\begin{aligned} \hat{F}'^{(n_B)}_{\text{no-click}} &:= {}_{EE'}\langle \mathrm{vac}|\,\hat{U}^\dagger \hat{F}^{(n_B)}_{\text{no-click}} \hat{U}\,|\mathrm{vac}\rangle_{EE'} \\ &= (1-d)^4 p_L^{n_B}\hat{\mathbb{1}}^{(n_B)}_B. \end{aligned} \quad (55)$$

By using Eqs. (45) and (53)–(55), we describe Eq. (41) in terms of system B:

$$\begin{aligned} \hat{F}'^{(n_B)}_{\text{cross}} &:= {}_{EE'}\langle \mathrm{vac}|\,\hat{U}^\dagger \hat{F}^{(n_B)}_{\text{cross}} \hat{U}\,|\mathrm{vac}\rangle_{EE'} \\ &= \hat{\mathbb{1}}^{(n_B)}_B - \hat{F}'^{(n_B)}_Z - \hat{F}'^{(n_B)}_X - \hat{F}'^{(n_B)}_{\text{no-click}} \\ &= \{1-(1-d)^2[(p_{Z'}+p_L)^{n_B} + (p_{X'}+p_L)^{n_B} \\ &\quad - (1-d)^2 p_L^{n_B}]\}\hat{\mathbb{1}}^{(n_B)}_B. \end{aligned} \quad (56)$$

From Eq. (53), the probability $s_{Z|n_B}$ that Bob obtains a Z-basis key under the condition that the QND measurement outcome is n_B is independent of the state of system B, which is

$$s_{Z|n_B} = (1-d)^2[(p_{Z'}+p_L)^{n_B} - (1-d)^2 p_L^{n_B}] \quad (57)$$

for arbitrary n_B. From Eq. (56), the probability $s_{\text{cross}|n_B}$ that the cross click occurs under the condition that the QND measurement outcome is n_B is also independent of the state of system B, which is

$$\begin{aligned} s_{\text{cross}|n_B} &= 1-(1-d)^2[(p_{Z'}+p_L)^{n_B} + (p_{X'}+p_L)^{n_B} \\ &\quad - (1-d)^2 p_L^{n_B}] \end{aligned} \quad (58)$$

for arbitrary n_B.

In a round with Alice's photon number $n_A = 1$, from Eq. (7), she is considered to send the state $|\Phi^{(1)}_Z\rangle_{AA'}$ to Bob regardless of her basis choice, and thus the outcome n_B of Bob's QND measurement is independent of Alice's basis choice. On the other hand, the probability of Bob's passive basis choice depends only on photon number n_B, as shown in Eq. (57). These imply that Alice's basis choice and Bob's passive basis choice are independent. Therefore, in a round where Alice emits a single photon and Bob receives n_B photons, the probability that a Z-basis sifted key is generated is $p_Z s_{Z|n_B}$. This equals $Q^{(1,n_B)}_Z/Q^{(1,n_B)}$ in the asymptotic limit, that is, $Q^{(1,n_B)}_Z/Q^{(1,n_B)} \sim p_Z s_{Z|n_B}$. Similarly, $Q^{(1,n_B)}_{\text{cross}}/Q^{(1,n_B)} \sim s_{\text{cross}|n_B}$ also holds. Thus,

$$
\begin{aligned}
Q_Z^{(1,n_B)} &\sim \frac{p_Z s_{Z|n_B}}{s_{\mathrm{cross}|n_B}} Q_{\mathrm{cross}}^{(1,n_B)} \\
&= \frac{p_Z[(p_{Z'}+p_L)^{n_B} - (1-d)^2 p_L^{n_B}](1-d)^2 Q_{\mathrm{cross}}^{(1,n_B)}}{1-[(p_{Z'}+p_L)^{n_B} + (p_{X'}+p_L)^{n_B} - (1-d)^2 p_L^{n_B}](1-d)^2} \\
&= \frac{p_Z[(p_{Z'}+p_L)^{n_B} - (1-d)^2 p_L^{n_B}] Q_{\mathrm{cross}}^{(1,n_B)}}{1/(1-d)^2 - [(p_{Z'}+p_L)^{n_B} + (p_{X'}+p_L)^{n_B} - (1-d)^2 p_L^{n_B}]} \\
&\le \frac{p_Z[(p_{Z'}+p_L)^{n_B} - (1-d)^2 p_L^{n_B}] Q_{\mathrm{cross}}^{(1,n_B)}}{1-[(p_{Z'}+p_L)^{n_B} + (p_{X'}+p_L)^{n_B} - (1-d)^2 p_L^{n_B}]} \\
&\le \frac{p_Z (p_{Z'}+p_L)^{n_B} Q_{\mathrm{cross}}^{(1,n_B)}}{1-[(p_{Z'}+p_L)^{n_B} + (p_{X'}+p_L)^{n_B}]}.
\end{aligned} \tag{59}
$$

Since $p_{Z'}+p_L < 1$ and $p_{X'}+p_L < 1$ hold, for any $n_B \ge 2$, we have

$$
Q_Z^{(1,n_B)} \lesssim \alpha Q_{\mathrm{cross}}^{(1,n_B)}, \tag{60}
$$

where

$$
\alpha := \frac{p_Z (p_{Z'}+p_L)^2}{1-[(p_{Z'}+p_L)^2 + (p_{X'}+p_L)^2]}. \tag{61}
$$

By defining a quantity

$$
Q_{\mathrm{cross}}^{(n_A=1)} := \sum_{n_B \ge 0} Q_{\mathrm{cross}}^{(1,n_B)}, \tag{62}
$$

which can be estimated with the decoy-state method, Eq. (60) leads to

$$
\sum_{n_B \ge 2} Q_Z^{(1,n_B)} \lesssim \alpha Q_{\mathrm{cross}}^{(n_A=1)}. \tag{63}
$$

By substituting this into Eq. (35), we obtain

$$
\begin{aligned}
f_{\mathrm{PA}}^{\mathrm{alt}} \lesssim\ & Q_Z - Q_Z^{(n_A=0)} - (Q_Z^{(n_A=1)} - \alpha Q_{\mathrm{cross}}^{(n_A=1)}) \\
& \times \left(1 - h\left(\frac{p_Z \tilde{p}_Z E_X^{(n_A=1)}}{p_X \tilde{p}_X (Q_Z^{(n_A=1)} - \alpha Q_{\mathrm{cross}}^{(n_A=1)})}\right)\right).
\end{aligned} \tag{64}
$$

C. Estimation with decoy-state method

Here we derive bounds on the parameters $E_X^{(n_A=1)}$, $Q_Z^{(n_A=0)}$, $Q_Z^{(n_A=1)}$, and $Q_{\mathrm{cross}}^{(n_A=1)}$ in Eq. (64), which are mentioned in the previous sections as values that can be evaluated with the decoy-state method. As described in the actual protocol, the decoy-state method with weak coherent states and the vacuum is used. In Appendix B, we confirm that the decoy-state method can be applied to the passive protocol in a similar way to the active protocol [27]. A difference from the active protocol is that we estimate the cross-click rate with the decoy-state method as well. The result is as follows:

$$
\begin{aligned}
Q_Z^{(n_A=0)} &\gtrsim \underline{Q}_Z^{(n_A=0)} \\
&:= (p_\mu e^{-\mu} + p_\nu e^{-\nu} + p_0) Q_{Z|0}, \\
Q_Z^{(n_A=1)} &\gtrsim \underline{Q}_Z^{(n_A=1)} \\
&:= \frac{\mu(p_\mu e^{-\mu}\mu + p_\nu e^{-\nu}\nu)}{\mu\nu - \nu^2} \\
&\quad \times \left(Q_{Z|\nu} e^{\nu} - Q_{Z|\mu} e^{\mu} \frac{\nu^2}{\mu^2} - Q_{Z|0} \frac{\mu^2 - \nu^2}{\mu^2}\right), \\
E_X^{(n_A=1)} &\lesssim \bar{E}_X^{(n_A=1)} \\
&:= (p_\mu e^{-\mu}\mu + p_\nu e^{-\nu}\nu) \frac{E_{X|\nu} e^{\nu} - E_{X|0}}{\nu}, \\
Q_{\mathrm{cross}}^{(n_A=1)} &\lesssim \bar{Q}_{\mathrm{cross}}^{(n_A=1)} \\
&:= (p_\mu e^{-\mu}\mu + p_\nu e^{-\nu}\nu) \frac{Q_{\mathrm{cross}|\nu} e^{\nu} - Q_{\mathrm{cross}|0}}{\nu}.
\end{aligned} \tag{65}
$$

We can see that all parameters on the right-hand side are known in advance or observed after the implementation.

D. Secure key rate

Now we derive the secure key rate based on the results so far. By combining Eq. (64) with Eq. (65), if we set

$$
\begin{aligned}
f_{\mathrm{PA}} =\ & Q_Z - \underline{Q}_Z^{(n_A=0)} - (\underline{Q}_Z^{(n_A=1)} - \alpha \bar{Q}_{\mathrm{cross}}^{(n_A=1)}) \\
& \times \left(1 - h\left(\frac{p_Z \tilde{p}_Z \bar{E}_X^{(n_A=1)}}{p_X \tilde{p}_X (\underline{Q}_Z^{(n_A=1)} - \alpha \bar{Q}_{\mathrm{cross}}^{(n_A=1)})}\right)\right),
\end{aligned} \tag{66}
$$

the alternative protocol is secure, i.e., the actual protocol is also secure. Therefore, the key generation rate per

nonsampling round is given by

$$R = Q_Z - f_{\mathrm{PA}} - f_{\mathrm{EC}} = \underline{Q}_Z^{(n_A=0)} + (\underline{Q}_Z^{(n_A=1)} - \alpha \bar{Q}_{\mathrm{cross}}^{(n_A=1)}) \times \left(1 - h\left(\frac{p_Z \tilde{p}_Z \bar{E}_X^{(n_A=1)}}{p_X \tilde{p}_X (\underline{Q}_Z^{(n_A=1)} - \alpha \bar{Q}_{\mathrm{cross}}^{(n_A=1)})}\right)\right) - f_{\mathrm{EC}} \tag{67}$$

as long as $R > 0$ and the following inequality is satisfied:

$$\frac{p_Z \tilde{p}_Z}{p_X \tilde{p}_X} \bar{E}_X^{(n_A=1)} \leq \frac{1}{2}(\underline{Q}_Z^{(n_A=1)} - \alpha \bar{Q}_{\mathrm{cross}}^{(n_A=1)}). \tag{68}$$

Note that Eq. (68) is a sufficient condition for Eq. (33) because $E_X^{(n_A=1)} \lesssim \bar{E}_X^{(n_A=1)}$ and $q_Z = Q_Z^{(n_A=1)} - \sum_{n_B \geq 2} Q_Z^{(1,n_B)} \gtrsim \underline{Q}_Z^{(n_A=1)} - \alpha \bar{Q}_{\mathrm{cross}}^{(n_A=1)}$ hold from Eqs. (63) and (65).

IV. NUMERICAL ANALYSIS

In this section, we simulate the secure key rate with realistic parameters for experiments to compare the active and passive protocols. We also show that the bounds in our security proof are tight enough under such a realistic situation.

A. Simulation of secure key rate

We show results of numerical calculation of the key rate R per nonsampling round given by Eq. (67). In the simulation shown in Fig. 4, we assume detectors' quantum efficiency $\eta_{\mathrm{det}}^Z = \eta_{\mathrm{det}}^X = 0.7$ and dark-count probability $d = 10^{-7}$, which are achievable with commercial superconducting single-photon detectors [28]. The overall transmittances of the Z line and X line are $\eta_Z = \eta_{\mathrm{det}}^Z$ and $\eta_X = \eta_{\mathrm{det}}^X r$, respectively. The channel transmittance of the optical fiber η_{ch} connecting Alice and Bob is modeled as $\eta_{\mathrm{ch}} = 10^{-l/50}$, where l indicates its length (km). The bit error rates e_Z and e_X of the Z basis and X basis, respectively, are calculated from the dark count rate in addition to the channel error rate $e_{\mathrm{ch}} = 0.03$. The cost for error correction f_{EC} is $c_{\mathrm{EC}} Q_Z h(e_Z)$, where the error-correction coefficient c_{EC} is set to be 1.1 [29].

Regarding the decoy-state method, we assume $p_\mu \to 1$ because ratios using the decoy intensities ν and 0 can be negligibly small in the asymptotic limit of $m_{\mathrm{rep}} \to \infty$. The decoy intensity ν is fixed to be 0.05. Optimizing signal intensity μ and the probability p_Z at each distance, in Fig. 4(a), we plot numerical results for three cases: (i) a secure key rate of the active biased BB84 protocol for comparison (green), (ii) our result R with $r = 1$ (blue), and (iii) our result R with $r = 0.5$ (red). The vertical axis is on a logarithmic scale with base 10. In Fig. 4(b), we plot the optimal values of p_Z as a function of the fiber length. The value p_Z is optimized in the range of $[0.5, 0.99]$ in increments of 0.01.

Furthermore, assuming a more conservative scenario, in Figs. 5(a) and 5(b), we plot numerical results under the same conditions as in Fig. 4 except with the quantum efficiency $\eta_{\mathrm{det}}^Z = \eta_{\mathrm{det}}^X = 0.2$ and the dark-count probability

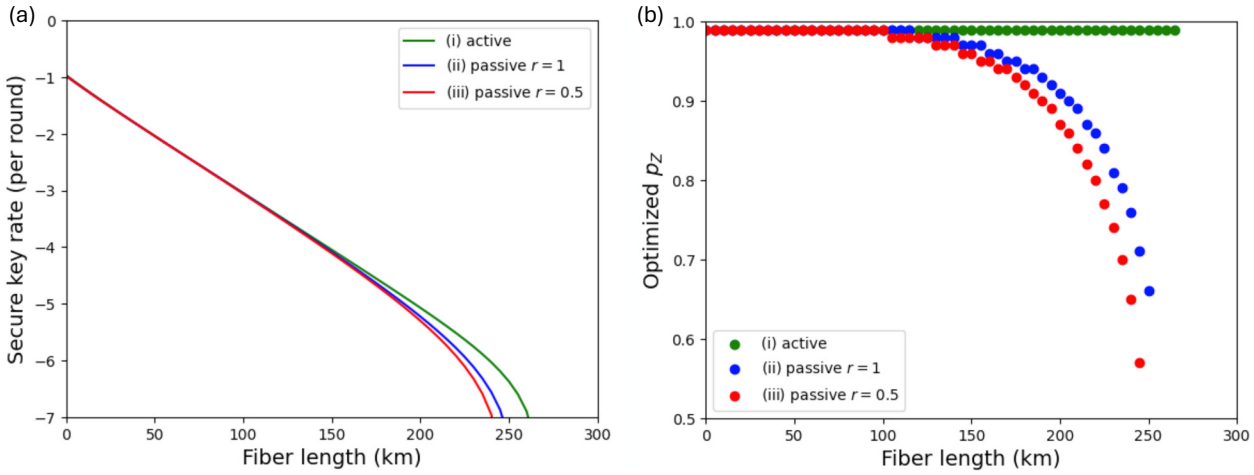


FIG. 4. Secure key rate and the optimal probability of the basis choice as a function of fiber length with the quantum efficiency $\eta_{\mathrm{det}}^Z = \eta_{\mathrm{det}}^X = 0.7$ and the dark-count probability $d = 10^{-7}$ of detectors. (a) Secure key rate R per round on a logarithmic scale with base 10 as a function of fiber length (km). The top line (green) is the secure key rate of the active biased protocol for comparison. The middle line (blue) is our result R for the passive biased protocol with $r = 1$ representing the symmetry of transmittance between the Z line and X line. The bottom line (red) is R with $r = 1/2$. We assume that the intensity of a weak coherent decoy state is $\nu = 0.05$, the channel error rate is $e_{\mathrm{ch}} = 0.03$, and the error-correction coefficient is $c_{\mathrm{EC}} = 1.1$. The probability p_Z and the signal intensity μ are optimized at each distance. (b) Optimal p_Z as a function of fiber length (km). The value p_Z is optimized in the range of $[0.5, 0.99]$ in increments of 0.01.

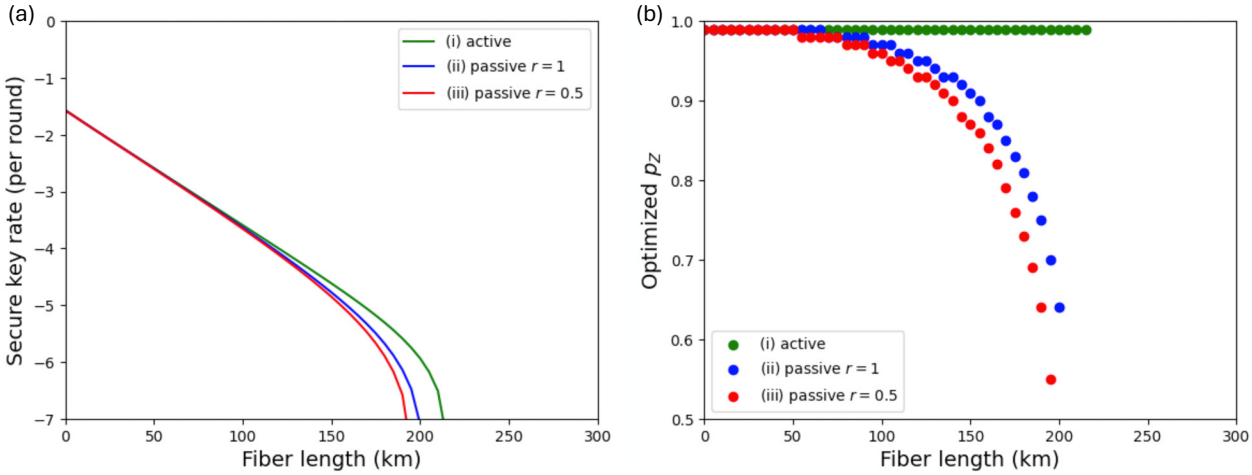


FIG. 5. Secure key rate and the optimal probability of the basis choice as a function of fiber length with the quantum efficiency $\eta^Z_{\rm def} = \eta^X_{\rm det} = 0.2$ and the dark-count probability $d = 3 \times 10^{-7}$ of detectors. The other conditions are the same as those in Fig. 4.

$d = 3 \times 10^{-7}$, which are achievable with current single-photon avalanche diode technology [30].

As shown in both Figs. 4 and 5, there is an intrinsic gap between active case (i) and passive case (ii), which implicates the vulnerability of the passive basis choice to dark counts. To explain this, let us consider the signal-to-noise ratio (SNR), where noise is generated from the dark counts of the detectors. The secure key cannot be generated when the order of the SNR is 1 because it induces a large error rate. For the active biased protocol, in which the same setup is used for the Z basis and X basis except for the wave plate to change the basis, the SNR is independent of the basis choice. On the other hand, for the passive biased protocol, in which a signal is divided into the Z line and X line corresponding to the passive basis choice, the signal (and thus the SNR) in the X basis is smaller than in the active case by the factor of $p_X r$. Thus, in the range of long distances where the dark count rate is comparable to the signal in the X basis, to avoid the SNR approaching the order of 1, one must make p_X larger, i.e., p_Z smaller, which leads to a lower key generation rate in the Z basis.

The difference between case (ii) and case (iii) is also explained in the same manner, that is, a small r leads to a small SNR in the X basis. These intuitions are supported by the results in Figs. 4(b) and 5(b), in which the optimal value of p_Z decreases with fiber length in the passive case while it is fixed to be high in the active case.

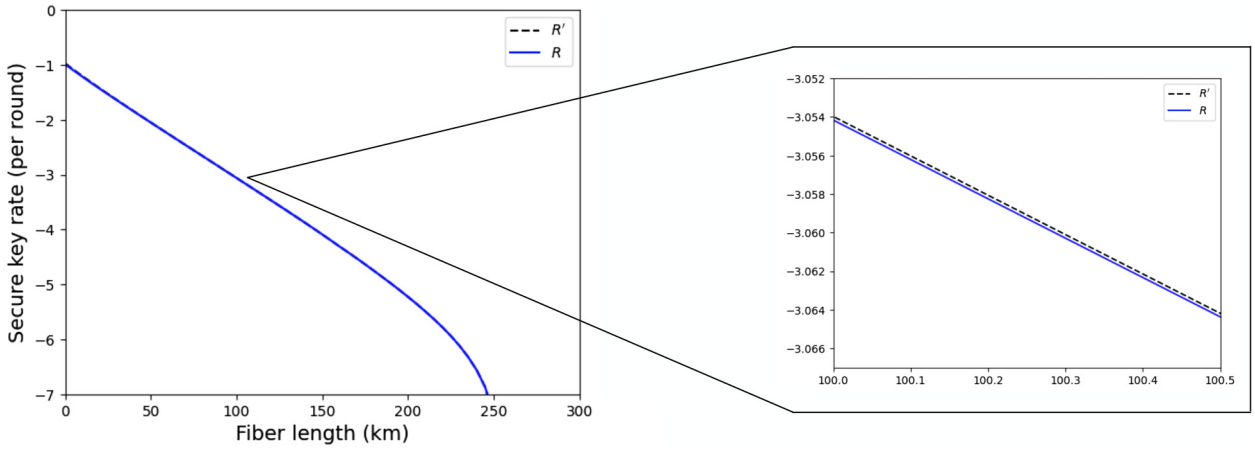


FIG. 6. Secure key rate R and virtual rate R' given by Eq. (69) on a logarithmic scale with base 10 as a function of fiber length (km). The blue solid line is the secure key rate R of our result with $r = 1$. The black dashed line is the virtual rate R' with $r = 1$, in which we assume that all incoming signals contain no more than one photon. The parameter setting for calculation is the same as that of Fig. 4. The probability p_Z and the signal intensity μ are optimized at each distance.

B. Tightness of our bounds

Although our security proof focuses only on Bob's single-photon detection events and discards multiple-photon events for simplicity, this does not significantly affect the key rate in practice. We emphasize that the decoy-state method enables us to obtain the upper bound $\bar{Q}_{\mathrm{cross}}^{(n_A=1)}$ on the ratio $Q_{\mathrm{cross}}^{(n_A=1)}$ of the number of cross-click rounds with Alice's single-photon emission to the number of nonsampling rounds. Since multiple photons do not arrive at Bob's site in rounds with Alice's single-photon emission as long as Eve does not intentionally insert multiple photons, cross-click events are induced by the dark counts of the detectors. That is, $\bar{Q}_{\mathrm{cross}}^{(n_A=1)} = \max\{O(\eta d), O(d^2)\}$, which is negligible compared to the lower bound on the sifted key rate $\underline{Q}_Z^{(n_A=1)} = O(\eta)$, where η represents the overall transmittance including the channel transmittance and the quantum efficiency. Thus, $\underline{Q}_Z^{(n_A=1)} - \alpha\bar{Q}_{\mathrm{cross}}^{(n_A=1)}$ in Eq. (67) is expected to almost equal $\underline{Q}_Z^{(n_A=1)}$.

In order to confirm the discussion here, we consider the virtual rate R' described as

$$R' := \underline{Q}_Z^{(n_A=0)} + \underline{Q}_Z^{(n_A=1)}\left(1 - h\left(\frac{p_Z\tilde{p}_Z\bar{E}_X^{(n_A=1)}}{p_X\tilde{p}_X\underline{Q}_Z^{(n_A=1)}}\right)\right) - f_{\mathrm{EC}}, \tag{69}$$

in which $\alpha\bar{Q}_{\mathrm{cross}}^{(n_A=1)}$ is removed from Eq. (67). This corresponds to an optimistic assumption that all incoming signals to Bob contain no more than one photon. With the parameters used in Sec. IV A and setting $r = 1$, we calculated R and R' to compare them, as shown in Fig. 6. The vertical axis is on a logarithmic scale with base 10. As expected, we can see that the difference between R and R' is negligible.

V. CONCLUSION

Here we have proved the security of the decoy-state BB84 protocol with receiver's passive biased basis choice in the asymptotic limit. The difficulty stems from the fact that the probability of basis choice depends on the incoming photon number. We have overcome the problem by estimating the contribution of multiple photons from the ratio of cross-click rounds, to limit our analysis to Bob's single-photon space, combined with a security proof based on complementarity. The numerical results show that, thanks to the application of the decoy-state method to cross-click events, the passive protocol achieves a key generation rate comparable to that of the active protocol, except at long distances.

Although this work has focused on the security proof in the asymptotic limit, it can be extended to a finite-key analysis using concentration inequalities such as Kato's inequality [31]. On the other hand, since fully passive optical setups are effective in preventing side-channel attacks, a version of the BB84 protocol with passive setups on Alice's side was proposed, and its security has been proven [32–34]. In our work, Alice's state preparation is assumed to be performed actively rather than passively. To move toward fully passive QKD with a biased basis choice, it would be desirable to combine our work with their security proof. However, such integration is nontrivial and is left as an open problem for future work.

Note added.—After the completion of this work, a related study was presented by Wang *et al.* [35]. Their work can be seen as a generalization of ours, in the sense that it incorporates finite-key effects and considers various device imperfections, such as quantum efficiency mismatch in the Z (or X) line. However, to the best of our knowledge, our work provides the first analytical security proof of the passive biased BB84 protocol in the asymptotic limit.

ACKNOWLEDGMENTS

We thank Akihiro Mizutani, Kiyoshi Tamaki, Takuya Ikuta, Toshimori Honjo, Lars Kamin, and Devashish Tupkary for helpful discussions. We are grateful for support from the MIC R&D of ICT Priority Technology (Grant No. JPMI00316) of the Ministry of Internal Affairs and Communications of Japan.

DATA AVAILABILITY

The data that support the findings of this article are not publicly available upon publication because it is not technically feasible and/or the cost of preparing, depositing, and hosting the data would be prohibitive within the terms of this research project. The data are available from the authors upon reasonable request.

APPENDIX A: THEORETICAL DIFFERENCE BETWEEN ACTIVE AND PASSIVE BASIS CHOICE

Here we show the qualitative difficulty of the passive biased BB84 protocol from the perspective of a security proof. We assume that optical loss is balanced between the Z line and X line (i.e., $r = 1$) and there is no dark count for simplicity. Let us denote $Q_X^{(n_A=1)} := \sum_{n_B\geq 0} Q_X^{(1,n_B)}$.

For the active biased protocol,

$$E_{\mathrm{ph}}^{(1,n_B)} \sim \frac{p_Z^2}{p_X^2}E_X^{(1,n_B)} \quad \text{and} \quad Q_Z^{(1,n_B)} \sim \frac{p_Z^2}{p_X^2}Q_X^{(1,n_B)} \tag{A1}$$

hold for any n_B in the asymptotic limit because, when $n_A = 1$, Alice prepares the state $|\Phi_Z^{(1)}\rangle_{AA'}$ in Eq. (7) and sends system A' to Bob, followed by their basis choice

according to the probability distribution (p_Z, p_X). Thus, in the asymptotic limit, the phase error rate $e_{\rm ph}^{(n_A=1)} := E_{\rm ph}^{(n_A=1)}/Q_Z^{(n_A=1)}$ for $n_A = 1$ equals the observed error rate in the X basis:

$$e_{\rm ph}^{(n_A=1)} = \frac{E_{\rm ph}^{(n_A=1)}}{Q_Z^{(n_A=1)}} = \frac{\sum_{n_B\geq 0} E_{\rm ph}^{(1,n_B)}}{\sum_{n_B\geq 0} Q_Z^{(1,n_B)}} \sim \frac{(p_Z^2/p_X^2)\sum_{n_B\geq 0} E_X^{(1,n_B)}}{(p_Z^2/p_X^2)\sum_{n_B\geq 0} Q_X^{(1,n_B)}} = \frac{E_X^{(n_A=1)}}{Q_X^{(n_A=1)}}. \tag{A2}$$

On the other hand, if Bob chooses his basis passively (and assigns no bit to cross-click rounds), Bob's basis is conclusive only when all n_B photons go to the Z line or X line. The ratio of Z basis to X basis is $p_Z^{n_B} : p_X^{n_B}$ depending on n_B. Since Alice actively chooses her basis according to the probability distribution (p_Z, p_X),

$$E_{\rm ph}^{(1,n_B)} \sim \frac{p_Z^{n_B+1}}{p_X^{n_B+1}} E_X^{(1,n_B)} \quad \text{and} \quad Q_Z^{(1,n_B)} \sim \frac{p_Z^{n_B+1}}{p_X^{n_B+1}} Q_X^{(1,n_B)} \tag{A3}$$

hold in the asymptotic limit. The phase error rate for rounds with $n_A = 1$ is

$$e_{\rm ph}^{(n_A=1)} = \frac{E_{\rm ph}^{(n_A=1)}}{Q_Z^{(n_A=1)}} = \frac{\sum_{n_B\geq 0} E_{\rm ph}^{(1,n_B)}}{\sum_{n_B\geq 0} Q_Z^{(1,n_B)}} \sim \frac{\sum_{n_B\geq 0}(p_Z^{n_B+1}/p_X^{n_B+1}) E_X^{(1,n_B)}}{\sum_{n_B\geq 0}(p_Z^{n_B+1}/p_X^{n_B+1}) Q_X^{(1,n_B)}}, \tag{A4}$$

which is not identical to the X-basis error rate $E_X^{(n_A=1)}/Q_X^{(n_A=1)}$ for $n_A = 1$ except in the case of balanced basis choice, i.e., $p_Z = p_X = 1/2$.

As a consequence, if we consider the sum of all n_B mentioned in the above scenario, the relation, Eq. (A2), between the phase error and the X-basis error which is satisfied in the active protocol does not hold. This motivates us to analyze the security with fixed n_B to accomplish a simple proof.

APPENDIX B: DECOY STATE ANALYSIS FOR RECEIVER'S PASSIVE SETUP

Here we derive bounds on $Q_Z^{(n_A=0)}$, $Q_Z^{(n_A=1)}$, $E_X^{(n_A=1)}$, and $Q_{\rm cross}^{(n_A=1)}$ with decoy-state method using weak coherent states and the vacuum. In a similar way to Ref. [27], we first derive those bounds with intensities $\mu_A \in \{\mu, \nu_1, \nu_2\}$ satisfying $0 \leq \nu_2 < \nu_1$ and $\nu_1 + \nu_2 < \mu$, followed by taking $\nu_2 = 0$ at last. Let $Y_{Z|n'_A}$, $Y_{X|n'_A}^{\rm error}$, and $Y_{{\rm cross}|n'_A}$ be

$$\begin{aligned} Y_{Z|n'_A} &:= \frac{m(y_B = 1 \wedge W_A = W_B = Z \wedge n_A = n'_A)}{m(n_A = n'_A)}, \\ Y_{X|n'_A}^{\rm error} &:= \frac{m(y_B = 1 \wedge W_A = W_B = X \wedge n_A = n'_A \wedge b_A \neq b_B)}{m(n_A = n'_A)}, \\ Y_{{\rm cross}|n'_A} &:= \frac{m(y_B = 1 \wedge W_B = \perp \wedge n_A = n'_A)}{m(n_A = n'_A)}, \end{aligned} \tag{B1}$$

respectively. For $\mu_A \in \{\mu, \nu_1, \nu_2\}$, the following relations hold:

$$Q_{Z|\mu_A} \sim \sum_{n_A\geq 0} Y_{Z|n_A} \frac{\mu_A^{n_A}}{n_A!} e^{-\mu_A}, \tag{B2}$$

$$E_{X|\mu_A} \sim \sum_{n_A\geq 0} Y_{X|n_A}^{\rm error} \frac{\mu_A^{n_A}}{n_A!} e^{-\mu_A}, \tag{B3}$$

$$Q_{{\rm cross}|\mu_A} \sim \sum_{n_A\geq 0} Y_{{\rm cross}|n_A} \frac{\mu_A^{n_A}}{n_A!} e^{-\mu_A}. \tag{B4}$$

From Eq. (B2) with $\mu_A = \nu_1$ and $\mu_A = \nu_2$, we obtain

$$\begin{aligned} &\nu_1 Q_{Z|\nu_2} e^{\nu_2} - \nu_2 Q_{Z|\nu_1} e^{\nu_1} \\ &\quad \sim (\nu_1 - \nu_2) Y_{Z|0} - \nu_1\nu_2 \sum_{n_A\geq 2} Y_{Z|n_A} \frac{\nu_1^{n_A-1} - \nu_2^{n_A-1}}{n_A!} \\ &\quad \leq (\nu_1 - \nu_2) Y_{Z|0}. \end{aligned} \tag{B5}$$

A lower bound on $Y_{Z|0}$ is given by

$$Y_{Z|0} \gtrsim Y_{Z|0}^{\rm low} := \max\left\{ \frac{\nu_1 Q_{Z|\nu_2} e^{\nu_2} - \nu_2 Q_{Z|\nu_1} e^{\nu_1}}{\nu_1 - \nu_2},\ 0 \right\}, \tag{B6}$$

which leads to

$$\begin{aligned} Q_Z^{(n_A=0)} &\sim (p_\mu P_\mu^{\text{Poisson}}(0) + p_{\nu_1} P_{\nu_1}^{\text{Poisson}}(0) \\ &\quad + p_{\nu_2} P_{\nu_2}^{\text{Poisson}}(0)) Y_{Z|0} \\ &\gtrsim (p_\mu e^{-\mu} + p_{\nu_1} e^{-\nu_1} + p_{\nu_2} e^{-\nu_2}) Y_{Z|0}^{\text{low}}. \end{aligned} \tag{B7}$$

Next, from Eq. (B2) with $\mu_A = \mu$,

$$Q_{Z|\mu} e^{\mu} \sim \sum_{n_A \geq 0} Y_{Z|n_A} \frac{\mu^{n_A}}{n_A!} \tag{B8}$$

holds. The contribution of more than one photon is given by

$$\sum_{n_A \geq 2} Y_{Z|n_A} \frac{\mu^{n_A}}{n_A!} \sim Q_{Z|\mu} e^{\mu} - Y_{Z|0} - Y_{Z|1}\mu. \tag{B9}$$

We obtain the following inequality from Eq. (B2) with $\mu_A = \nu_1$ and $\mu_A = \nu_2$:

$$\begin{aligned} &Q_{Z|\nu_1} e^{\nu_1} - Q_{Z|\nu_2} e^{\nu_2} \\ &\sim Y_{Z|1}(\nu_1 - \nu_2) + \sum_{n_A \geq 2} \frac{Y_{Z|n_A}}{n_A!} (\nu_1^{n_A} - \nu_2^{n_A}) \\ &= Y_{Z|1}(\nu_1 - \nu_2) + \sum_{n_A \geq 2} \frac{Y_{Z|n_A}}{n_A!} \mu^{n_A} \left(\left(\frac{\nu_1}{\mu} \right)^{n_A} - \left(\frac{\nu_2}{\mu} \right)^{n_A} \right) \\ &\leq Y_{Z|1}(\nu_1 - \nu_2) + \frac{\nu_1^2 - \nu_2^2}{\mu^2} \sum_{n_A \geq 2} \frac{Y_{Z|n_A}}{n_A!} \mu^{n_A} \\ &\sim Y_{Z|1}(\nu_1 - \nu_2) + \frac{\nu_1^2 - \nu_2^2}{\mu^2} (Q_{Z|\mu} e^{\mu} - Y_{Z|0} - Y_{Z|1}\mu) \\ &\lesssim Y_{Z|1}(\nu_1 - \nu_2) + \frac{\nu_1^2 - \nu_2^2}{\mu^2} (Q_{Z|\mu} e^{\mu} - Y_{Z|0}^{\text{low}} - Y_{Z|1}\mu) \\ &= \left(\nu_1 - \nu_2 - \frac{\nu_1^2 - \nu_2^2}{\mu} \right) Y_{Z|1} \\ &\quad + \frac{\nu_1^2 - \nu_2^2}{\mu^2} (Q_{Z|\mu} e^{\mu} - Y_{Z|0}^{\text{low}}), \end{aligned} \tag{B10}$$

where the first inequality is satisfied because $a^i - b^i \leq a^2 - b^2$ holds for $i \geq 2$ if $0 < a + b < 1$ and $\nu_1 + \nu_2 < \mu$ are assumed, and the third equality holds from Eq. (B9). Thus a lower bound on $Y_{Z|1}$ is given by

$$\begin{aligned} Y_{Z|1} &\gtrsim \frac{\mu}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2} \\ &\quad \times \left(Q_{Z|\nu_1} e^{\nu_1} - Q_{Z|\nu_2} e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2} (Q_{Z|\mu} e^{\mu} - Y_{Z|0}^{\text{low}}) \right), \end{aligned} \tag{B11}$$

which leads to

$$\begin{aligned} Q_Z^{(n_A=1)} &\sim (p_\mu P_\mu^{\text{Poisson}}(1) + p_{\nu_1} P_{\nu_1}^{\text{Poisson}}(1) \\ &\quad + p_{\nu_2} P_{\nu_2}^{\text{Poisson}}(1)) Y_{Z|1} \\ &\gtrsim \frac{\mu(p_\mu \mu e^{-\mu} + p_{\nu_1} \nu_1 e^{-\nu_1} + p_{\nu_2} \nu_2 e^{-\nu_2})}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2} \\ &\quad \times \left(Q_{Z|\nu_1} e^{\nu_1} - Q_{Z|\nu_2} e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2} (Q_{Z|\mu} e^{\mu} - Y_{Z|0}^{\text{low}}) \right). \end{aligned} \tag{B12}$$

For the error ratio, from Eq. (B3) with $\mu_A = \nu_1$ and $\mu_A = \nu_2$, we obtain

$$\begin{aligned} E_{X|\nu_1} e^{\nu_1} &\sim Y_{X|0}^{\text{error}} + Y_{X|1}^{\text{error}} \nu_1 + \sum_{n_A \geq 2} Y_{X|n_A}^{\text{error}} \frac{\nu_1^{n_A}}{n_A!}, \\ E_{X|\nu_2} e^{\nu_2} &\sim Y_{X|0}^{\text{error}} + Y_{X|1}^{\text{error}} \nu_2 + \sum_{n_A \geq 2} Y_{X|n_A}^{\text{error}} \frac{\nu_2^{n_A}}{n_A!}. \end{aligned} \tag{B13}$$

Since $\nu_1 > \nu_2$ is satisfied,

$$Y_{X|1}^{\text{error}} \lesssim \frac{E_{X|\nu_1} e^{\nu_1} - E_{X|\nu_2} e^{\nu_2}}{\nu_1 - \nu_2} \tag{B14}$$

holds, which leads to

$$\begin{aligned} &E_X^{(n_A=1)} \\ &\sim (p_\mu P_\mu^{\text{Poisson}}(1) + p_{\nu_1} P_{\nu_1}^{\text{Poisson}}(1) + p_{\nu_2} P_{\nu_2}^{\text{Poisson}}(1)) Y_{Z|1}^{\text{error}} \\ &\lesssim (p_\mu \mu e^{-\mu} + p_{\nu_1} \nu_1 e^{-\nu_1} + p_{\nu_2} \nu_2 e^{-\nu_2}) \frac{E_{X|\nu_1} e^{\nu_1} - E_{X|\nu_2} e^{\nu_2}}{\nu_1 - \nu_2}. \end{aligned} \tag{B15}$$

For the cross-click ratio, from Eq. (B4) with $\mu_A = \nu_1$ and $\mu_A = \nu_2$, we obtain

$$\begin{aligned} Q_{\text{cross}|\nu_1} e^{\nu_1} &\sim Y_{\text{cross}|0} + Y_{\text{cross}|1} \nu_1 + \sum_{n_A \geq 2} Y_{\text{cross}|n_A} \frac{\nu_1^{n_A}}{n_A!}, \\ Q_{\text{cross}|\nu_2} e^{\nu_2} &\sim Y_{\text{cross}|0} + Y_{\text{cross}|1} \nu_2 + \sum_{n_A \geq 2} Y_{\text{cross}|n_A} \frac{\nu_2^{n_A}}{n_A!}. \end{aligned} \tag{B16}$$

Since $\nu_1 > \nu_2$ is satisfied,

$$Y_{\text{cross}|1} \lesssim \frac{Q_{\text{cross}|\nu_1} e^{\nu_1} - Q_{\text{cross}|\nu_2} e^{\nu_2}}{\nu_1 - \nu_2} \tag{B17}$$

holds, which leads to

$$\begin{aligned} Q_{\mathrm{cross}}^{(n_A=1)} &\sim (p_\mu P_\mu^{\mathrm{Poisson}}(1) + p_{\nu_1} P_{\nu_1}^{\mathrm{Poisson}}(1) \\ &\quad + p_{\nu_2} P_{\nu_2}^{\mathrm{Poisson}}(1)) Y_{\mathrm{cross}|1} \\ &\lesssim (p_\mu \mu e^{-\mu} + p_{\nu_1} \nu_1 e^{-\nu_1} + p_{\nu_2} \nu_2 e^{-\nu_2}) \\ &\quad \times \frac{Q_{\mathrm{cross}|\nu_1} e^{\nu_1} - Q_{\mathrm{cross}|\nu_2} e^{\nu_2}}{\nu_1 - \nu_2}. \end{aligned} \tag{B18}$$

In Eqs. (B7), (B12), (B15), and (B18), by taking $\nu_1 = \nu$ and $\nu_2 = 0$, we obtain Eq. (65).

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE Press, New York, 1984), Vol. 175.

[2] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, Phys. Rev. Lett. **91**, 057901 (2003).

[3] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[4] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[5] X.-B. Wang, Decoy-state protocol for quantum cryptography with four different intensities of coherent light, Phys. Rev. A **72**, 012322 (2005).

[6] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Squashing models for optical measurements in quantum communication, Phys. Rev. Lett. **101**, 093601 (2008).

[7] T. Tsurumaru and K. Tamaki, Security proof for quantum-key-distribution systems with threshold detectors, Phys. Rev. A **78**, 032302 (2008).

[8] M. Koashi, Efficient quantum key distribution with practical sources and detectors, ArXiv:quant-ph/0609180.

[9] M. Koashi, Simple security proof of quantum key distribution based on complementarity, New J. Phys. **11**, 045018 (2009).

[10] M. Tomamichel and R. Renner, Uncertainty relation for smooth entropies, Phys. Rev. Lett. **106**, 110506 (2011).

[11] H.-K. Lo, H. Chau, and M. Ardehali, Efficient quantum key distribution scheme and a proof of its unconditional security, J. Cryptol. **18**, 133 (2004).

[12] S.-K. Liao, *et al.*, Satellite-to-ground quantum key distribution, Nature **549**, 43 (2017).

[13] S. Sivasankaran, C. Liu, M. Mihm, and A. Ling, in *2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS)* (IEEE, Kyoto, Japan, 2022), p. 51.

[14] T. Roger, R. Singh, C. Perumangatt, D. G. Marangon, M. Sanzaro, P. R. Smith, R. I. Woodward, and A. J. Shields, Real-time gigahertz free-space quantum key distribution within an emulated satellite overpass, Sci. Adv. **9**, eadj5873 (2023).

[15] Y. Li, *et al.*, Microsatellite-based real-time quantum key distribution, Nature **640**, 47 (2025).

[16] H.-L. Yin, P. Liu, W.-W. Dai, Z.-H. Ci, J. Gu, T. Gao, Q.-W. Wang, and Z.-Y. Shen, Experimental composable security decoy-state quantum key distribution using time-phase encoding, Opt. Express **28**, 29479 (2020).

[17] D. Scalcon, C. Agnesi, M. Avesani, L. Calderaro, G. Foletto, A. Stanco, G. Vallone, and P. Villoresi, Cross-encoded quantum key distribution exploiting time-bin and polarization states with qubit-based synchronization, Adv. Quantum Technol. **5**, 2200051 (2022).

[18] Y.-L. Tang, *et al.*, Time-bin phase-encoding quantum key distribution using Sagnac-based optics and compatible electronics, Opt. Express **31**, 26335 (2023).

[19] F. Grünenfelder, A. Boaron, G. V. Resta, M. Perrenoud, D. Rusca, C. Barreiro, R. Houlmann, R. Sax, L. Stasi, S. El-Khoury, E. Hänggi, N. Bosshard, F. Bussières, and H. Zbinden, Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems, Nat. Photonics **17**, 422 (2023).

[20] S. Francesconi, C. De Lazzari, D. Ribezzo, I. Vagniluca, N. Biagi, T. Occhipinti, A. Zavatta, and D. Bacco, Scalable implementation of temporal and phase encoding QKD with phase-randomized states, Adv. Quantum Technol. **7**, 2300224 (2024).

[21] L. Kamin and N. Lütkenhaus, Improved decoy-state and flag-state squashing methods, Phys. Rev. Res. **6**, 043223 (2024).

[22] D. Tupkary, E. Y. Z. Tan, S. Nahar, L. Kamin, and N. Lütkenhaus, QKD security proofs for decoy-state BB84: Protocol variations, proof techniques, gaps and limitations, ArXiv:2502.10340.

[23] Y. Zhang, P. J. Coles, A. Winick, J. Lin, and N. Lütkenhaus, Security proof of practical quantum key distribution with detection-efficiency mismatch, Phys. Rev. Res. **3**, 013076 (2021).

[24] L. Kamin, D. Tupkary, and N. Lütkenhaus, Improved finite-size effects in QKD protocols with applications to decoy-state QKD, ArXiv:2502.05382.

[25] L. Kamin, J. Burniston, and E. Y. Z. Tan, Rényi security framework against coherent attacks applied to decoy-state QKD, ArXiv:2504.12248.

[26] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on practical quantum cryptography, Phy. Rev. Lett. **85**, 1330 (2000).

[27] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).

[28] Y. Sanari, A. Taniguchi, M. Miura, H. Takahashi, K. Takasugi, H.-P. Lo, T. Ikuta, T. Honjo, and H. Takesue, in *2024 Conference on Lasers and Electro-Optics Pacific Rim (CLEO-PR)* (Optica Publishing Group, Incheon, Korea, 2024).

[29] Y. Luo, X. Cheng, H.-K. Mao, and Q. Li, An overview of postprocessing in quantum key distribution, Mathematics **12**, 2243 (2024).

[30] B. Li, Y. Niu, Y. Feng, and X. Chen, Ultra-low dark count InGaAs/InP single photon avalanche diode, Optoelectron. Lett. **18**, 647 (2022).

[31] G. Kato, Concentration inequality using unconfirmed knowledge, ArXiv:2002.04357.

[32] W. Wang, R. Wang, C. Hu, V. Zapatero, L. Qian, B. Qi, M. Curty, and H.-K. Lo, Fully passive quantum key distribution, Phys. Rev. Lett. **130**, 220801 (2023).

[33] V. Zapatero, W. Wang, and M. Curty, A fully passive transmitter for decoy-state quantum key distribution, Quantum Sci. Technol. **8**, 025014 (2023).

[34] V. Zapatero and M. Curty, Finite-key security of passive quantum key distribution, Phys. Rev. Appl. **21**, 014018 (2024).

[35] Z. Wang, D. Tupkary, and S. Nahar, Phase error estimation for passive detection setups with imperfections and memory effects, ArXiv:2508.21486.