Editors' Suggestion

# Quantum key distribution with basis-dependent detection probability

Federico Grasselli,[1,2,*] Giovanni Chesi,[3] Nathan Walk,[4] Hermann Kampermann,[1] Adam Widomski,[5] Maciej Ogrodnik,[5] Michał Karpiński,[5] Chiara Macchiavello,[3] Dagmar Bruß,[1] and Nikolai Wyderka[1,†]

[1] *Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, 40225 Düsseldorf, Germany*

[2] *Leonardo Innovation Labs—Quantum Technologies, Via Tiburtina km 12,400, 00131 Rome, Italy*

[3] *Physics Department, QUIT Group, University of Pavia, INFN Sezione di Pavia, Via Bassi 6, 27100 Pavia, Italy*

[4] *Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*

[5] *Faculty of Physics, University of Warsaw, Pasteura 5, 02-093 Warsaw, Poland*

(Received 9 December 2024; revised 3 February 2025; accepted 26 February 2025; published 4 April 2025)

Quantum key distribution (QKD) is a promising technology for secure communication. Nevertheless, QKD is still treated with caution in certain contexts due to potential gaps between theoretical models and actual QKD implementations. A common assumption in security proofs is that the detection probability at the receiver, for a given input state, is independent of the measurement basis, which might not always be verified and could lead to security loopholes. This paper presents a security proof for QKD protocols that does not rely on the aforementioned assumption and is thus applicable in scenarios with detection probability mismatches, even when induced by the adversary. We demonstrate, through simulations, that our proof can extract positive key rates for setups vulnerable to large detection probability mismatches. This is achieved by one monitoring whether an adversary is actively exploiting such vulnerabilities, instead of considering the worst-case scenario as in previous proofs. Our work highlights the importance of accounting for basis-dependent detection probabilities and provides a concrete solution for improving the security of practical QKD systems.

DOI: 10.1103/PhysRevApplied.23.044011

## I. INTRODUCTION

Quantum key distribution (QKD) is one of the most studied, developed, and commercialized quantum technologies of the past few decades [1]. With QKD, two users can, in principle, establish an information-theoretically secure key when linked by an insecure quantum channel and an authenticated classical channel [2], thereby providing a solution for long-term secure communication.

However, QKD is still facing some challenges that hinder its widespread adoption and standardization [3]. From a security point of view, the main challenge is the implementation security of QKD protocols [4,5], which arises due to a disagreement between the theoretical models used by the security proofs and the actual implementation of QKD protocols. Indeed, discrepancies between theory and experiment have been exploited to conduct successful quantum hacking attacks on QKD setups [6].

A crucial quantity in the security of prepare-and-measure QKD schemes with two measurement bases is the phase error rate [7]. In simple terms, this is the error rate in a basis complementary to the key basis— usually called the "test basis"—that characterizes the pulses detected in key generation rounds. Standard QKD security proofs assume that the detection probability of a given state is independent of the measurement basis [8–10], such that the phase error rate reduces to the (observed) bit error rate of the test measurements. However, this assumption is typically not verified by QKD experimental setups, potentially opening a security loophole that can be exploited by an eavesdropper.

A basis-dependent detection probability, or efficiency—we will use the two terms interchangeably—could originate from an asymmetry in the nominal efficiency or dark count probability of the detectors used in the two measurement bases [11,12]. The resulting mismatch in the detection probability of the two bases is typically independent of the optical mode incident upon the detector and

*Contact author: federico.grasselli@hhu.de
†Contact author: wyderka@hhu.de

can be easily characterized. On the other hand, a mode-dependent detection efficiency mismatch could originate from an asymmetric coupling of the two measurement bases to the incoming mode. A notable example is tailored light pulses prepared by the adversary to control which basis clicks in time-frequency QKD setups [13,14]. Regardless of the origin, a basis-dependent detection probability introduces a vulnerability in the QKD protocol that must be treated with hardware countermeasures or security proof fixes. Indeed, popular attacks on QKD systems, such as detector blinding attacks [15], time-shift attacks [16], and spatial-mode attacks on free-space QKD systems [17], can be traced back to basis-dependent detection probabilities.

In this work, we address the security of prepare-and-measure QKD protocols with basis-dependent detection probabilities. In particular, we derive an analytical security proof where the assumption about the independence of the detection probability of a state from the measurement basis is dropped. This implies that the phase error rate is no longer identified with the bit error rate in the test basis. Our proof directly applies to all QKD setups where one of the two measurements is a time-of-arrival measurement, e.g., time-bin QKD [18–21] and time-frequency QKD [13,22–27], but could also be extended to other setups. Our proof is obtained in the asymptotic regime and under collective attacks.

A key role in our solution is played by a high-speed tunable beam splitter (TBS) that is used by the receiver to redirect the signal to the two measurement bases. Our proof processes the rich measurement statistics enabled by the TBS with advanced techniques, including the detector decoy technique [28], to quantify the mismatch in the detection probability of the two bases and reduce the key rate accordingly.

We apply our proof to an experimental time-encoded QKD setup that is prone to efficiency mismatches [29,30] and show that it generates positive key rates for honest implementations. We then design a sophisticated attack that induces significant asymmetries in the detection efficiency of the two bases by preparing tailored pulses. We show that our proof reduces the key rate proportionately to the extent of the attack, while the standard BB84 key rate would return overly optimistic key rates due to its inability to detect the attack. Moreover, we argue that previous security proofs applicable to such scenarios would return pessimistic rates since they consider the worst-case scenario, i.e., the scenario of the attack, even when the eavesdropper is not present.

This paper is organized as follows. In Sec. II we discuss security loopholes and countermeasures linked to basis-dependent detection probabilities and describe an attack exploiting asymmetric nominal efficiencies. In Sec. III we illustrate a generic prepare-and-measure QKD protocol, which may feature basis-dependent detection probabilities. In Sec. IV we highlight the main points of the protocol's security proof, while we defer the fully detailed proof to Appendix C. In Sec. V we simulate the key rate of a time-encoded QKD scheme with our security proof both in an honest implementation and with attack-induced detection efficiency asymmetries. We provide further simulation details in Appendix E. We discuss the results of the simulations in Sec. VI and provide a summary in Sec. VII. In Appendix A we summarize the notation used in the paper, while in Appendix B we report the formula for the phase error rate resulting from our security proof. In Appendix D we derive some of the bounds required by our proof with the decoy-state method.

## II. SECURITY LOOPHOLES AND COUNTERMEASURES

Several proposed and implemented QKD schemes can present asymmetries in the detection probability of the two measurement bases, for certain input states. If their security proof fails to account for this fact, an eavesdropper could exploit the security loophole to invalidate the security claim on the established keys. In this paper, we adopt the common nomenclature of QKD for which Alice is the sender of the pulses and Bob the receiver, while Eve is the eavesdropper.

A mode-independent detection probability mismatch is easier to characterize and treat since the magnitude of the mismatch is independent of the light mode measured by Bob. It can be caused, for example, by detectors with unequal nominal efficiencies and/or unequal dark count probabilities. Nevertheless, here we provide an example where ignoring an asymmetry in the nominal detection efficiency of two detectors opens the door for a successful attack by Eve. To our knowledge, this type of attack was not listed in a recent report by the German cyber security agency (Bundesamt für Sicherheit in der Informationstechnik) about implementation attacks on QKD [31].

Consider the BB84 protocol where Bob has an active basis choice and, for simplicity, Alice has a deterministic single-photon source (the attack would also work with decoy BB84). Suppose that Eve performs an intercept-and-resend attack where she intercepts the signal and measures it in the $Z$ or $X$ basis, each with probability $p$, while she lets the signal go undisturbed with probability $1-2p$. Since Eve's attack generates noise in Bob's measurements, the key rate is reduced accordingly. In particular, the fraction of secret key bits in the sifted rounds is given by the BB84 asymptotic key rate:

$$r_{\mathrm{BB84}} = 1 - h(Q_X) - h(Q_Z). \tag{1}$$

If the $Z$-basis and $X$-basis detectors both have unit efficiency and if the quantum channel is ideal, except for

Eve's attack, the quantum bit error rate (QBER) in the two bases reads $Q_X = Q_Z = p/2$, where the factor $1/2$ accounts for the fact that when Eve's and Bob's bases differ, Bob's outcome is random. Suppose that the $X$-basis detector has efficiency $\eta_X$, with $\eta_X < 1$, while the $Z$-basis detector is still ideal. In this case, Eve performs the same attack as before, but this time she resends a pulse with $n$ photons (one photon) when she measures in the $X$ basis ($Z$ basis). This has the effect of spoiling the statistics of Bob's $X$-basis outcomes, by flooding them with events where there is no error since Eve's and Bob's bases agree, thereby decreasing the QBER in the $X$ basis. Indeed, the error probability in the $X$ basis is unchanged—the errors are still caused by the one photon sent by Eve when she chooses the wrong basis, i.e., the $Z$ basis—but the detection probability increases due to more photons arriving when Eve's and Bob's bases coincide. Overall, this decreases the QBER in the $X$ basis, which now reads

$$Q_X = \frac{p}{2}\left[1 + p\frac{1-\eta_X}{\eta_X}\left[1-(1-\eta_X)^{n-1}\right]\right]^{-1} < \frac{p}{2}. \quad (2)$$

On the other hand, $Q_Z$ remains unchanged by Eve's new attack, if we assume that multiclick events in the $Z$ basis are assigned randomly to one of the outcomes. As a consequence, the fraction of secret key bits in the sifted rounds, as per Eq. (1), increases compared with the case with ideal detectors, but Eve's knowledge of the key remains the same (indeed, note that the rounds discarded due to a no-click event in the $X$ basis are announced publicly, and hence are known to Eve). This implies that the key rate provided in the case of inefficient detectors is an overestimation of the actual secure key rate. The security of the key is thus compromised.

It is worth mentioning that security fixes in the case of detectors with mismatching nominal efficiencies have already been laid out, for example, in Refs. [11,12], for the BB84 protocol with an active basis choice.

Mismatching detection probabilities can also be a result of the different ways in which the two measurement bases are constructed. For instance, Ref. [18] features a two-dimensional time-bin encoding where the key basis measurement consists of a simple time-of-arrival measurement with a single-photon detector. Conversely, the test basis measurement is realized by an unbalanced Michelson interferometer with a delay in one of its arms, thereby spreading the whole signal over the range of three time bins, followed by a detector in only one of its output ports. This fact, combined with the fact that the outer time bins overlap with the bins of the neighboring rounds, implies that about 50% of potential detections are unobserved in the test basis compared with the key basis. This violates the basis-independent detection probability assumption of the security proofs [9,10] adopted in Ref. [18]. Similarly, in the BB84 protocols implemented in Refs. [19,32], the test basis measurement setup includes, among other optical elements, an interferometer where only one output is detected, such that the overall efficiency is reduced compared with that of the key basis measurements. By generalizing the setup in Ref. [18], Islam *et al.* [20] use a cascade of interferometers to detect the relative phases between pulses of a four-dimensional time-bin QKD protocol. Despite presenting a detector at each output port, they discard the detections in all but the central time bin, thus reducing the detection efficiency of the test basis by 75% under nominal conditions. In such setups [18,20], an attack analogous to the one described above, where Eve adds photons when measuring in the more lossy basis, would successfully spoil the security of the established key. Therefore, measures to avoid such attacks or modified security proofs are required to restore implementation security.

Mode-dependent detection probability mismatches depend on the coupling between the incoming light mode and each of the two measurement bases; hence, they might not emerge when the QKD experiment is operating nominally. Crucially, however, the assumption of a basis-independent detection probability must be verified not only by the experimental signals but also by any possible signal prepared by an adversary. For instance, prepare-and-measure protocols exploiting the complementarity of time and frequency (energy) degrees of freedom [13,22–27] are particularly prone to mode-dependent detection efficiency mismatches. In these setups the key basis is typically a time-of-arrival measurement, while the test basis consists of a frequency measurement. This is done either directly with spectrometers or indirectly through group delay dispersion. In the latter case, a dispersive medium spreads out a signal with differing delays depending on its frequency components, such that from the arrival time of a dispersed signal one can infer a frequency value. Regardless of the implemented frequency measurement, the finite detection windows in time and frequency represent a vulnerability that can be exploited by an eavesdropper. Indeed, as pointed out in Refs. [13,14], Eve can intercept the signals and measure either their time or their frequency, after which she prepares a very narrow pulse in time (if she measured the time) or in frequency (if she measured the frequency) and sends it to Bob. The detection probability of such signals at Bob strongly depends on the measurement basis. In the basis opposite to Eve's, the Fourier transform of a narrow pulse spreads out much more than the finite detection window of Bob's apparatus, thereby decreasing the detection probability significantly. This ensures that most of the detection events are those where Bob's choice and Eve's choice of basis match, hence invalidating security (unless no-detection events are kept).

Current security proofs that could account for mode-dependent detection probabilities are limited in scope and, more importantly, would return overly pessimistic

key rates [33–36]. In particular, the analytical proofs in Refs. [33,34] restrict Bob's input to be a single-photon signal, while the numerical security proof in Ref. [36] allows for multiphoton states received by Bob but assumes a deterministic single-photon source used by Alice. The main limitation of such proofs, however, is that they require a prior characterization of the mode-dependent detection efficiency of both measurement bases, for any possible incoming mode. Then, the worst-case efficiency mismatch between the two bases, among all potential input modes, determines the secure key rates given in Refs. [33–36]. Hence, the resulting key rates are overly pessimistic in all the practical scenarios where there is no eavesdropper tailoring the signals to those modes with the largest efficiency mismatch.

In contrast, our proof can handle both mode-independent and mode-dependent detection probability mismatches, it does not confine Alice's output or Bob's input to the single-photon subspace, and it is applicable to time-encoded QKD protocols such as the ones discussed in this section. Moreover, it can generate significantly higher key rates than previous proofs for honest implementations of protocols that are particularly sensitive to mode-dependent detection efficiency mismatches, e.g., time-frequency QKD (see Sec. VI).

## III. QKD PROTOCOL

We consider a prepare-and-measure QKD protocol with two measurement bases and $d$ outcomes per measurement. Bob measures the states sent by Alice with a measurement apparatus that is partially characterized. Namely, we assume that the mode-independent detection efficiencies (e.g., nominal detector efficiency, coupling loss) and the dark count probabilities of both measurement bases are known. Nevertheless, an imperfect characterization of such quantities would not affect security: any deviation between the characterized values and the setup's actual behavior will be treated by our proof as an attack attempt. Importantly, in contrast to previous proofs [33–36], we do not require a careful characterization of (possibly adversarial) mode-dependent efficiency mismatches.

### A. Alice's states

Alice prepares states from two sets, named the "$Z$-basis states" and the "$X$-basis states," respectively. The $Z$-basis states are primarily used for key generation, while the $X$-basis states are used for testing. In both bases, Alice prepares phase-randomized coherent states, as required by the decoy-state method [37–39], with three different intensities: $\mu_1$, $\mu_2$, and $\mu_3$. The three intensities satisfy $\mu_1 > \mu_2 + \mu_3$ and $\mu_2 > \mu_3 \geq 0$.

The $Z$-basis states form the set $\{\rho_{Z_j}\}_{j=0}^{d-1}$, where

$$\rho_{Z_j}(\mu_i) = \sum_{n=0}^{\infty} \Pr(n|\mu_i) |n_{Z_j}\rangle\langle n_{Z_j}| \tag{3}$$

is the state corresponding to the $j$th symbol of the $Z$ basis, with intensity $\mu_i$ $(i = 1, 2, 3)$. In Eq. (3) we defined the Fock state of $n$ photons in the mode of the $j$th symbol,

$$|n_{Z_j}\rangle := \frac{1}{\sqrt{n!}} \left(a^\dagger_{Z_j}\right)^n |\text{vac}\rangle , \tag{4}$$

where $a^\dagger_{Z_j}$ is the creation operator, as well as the Poissonian distribution of photons typical of phase-randomized coherent states,

$$\Pr(n|\mu_i) = e^{-\mu_i} \frac{\mu_i^n}{n!}. \tag{5}$$

The $X$-basis states are given by $\{\rho_{X_k}\}_{k=0}^{d-1}$, where

$$\rho_{X_k}(\mu_i) = \sum_{n=0}^{\infty} \Pr(n|\mu_i) |n_{X_k}\rangle\langle n_{X_k}| \tag{6}$$

is the state corresponding to the $k$th symbol of the $X$ basis, where $|n_{X_k}\rangle = (a^\dagger_{X_k})^n |\text{vac}\rangle / \sqrt{n!}$ is the Fock state of $n$ photons in the mode of the $k$th symbol and $a^\dagger_{X_k}$ is the creation operator. The only requirement on the states prepared by Alice is that their single-photon components do not reveal Alice's choice of basis to a potential eavesdropper. In other words, the average state prepared by Alice in the $Z$ and $X$ bases must coincide when restricted to the single-photon subspace [8,9]:

$$S := \sum_{j=0}^{d-1} |1_{Z_j}\rangle\langle 1_{Z_j}| = \sum_{k=0}^{d-1} |1_{X_k}\rangle\langle 1_{X_k}|. \tag{7}$$

This condition, satisfied by many QKD implementations (e.g., polarization, time bin), can be achieved if, for example, the two bases are linked by a discrete Fourier transform:

$$a^\dagger_{X_k} = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{\frac{-2\pi i}{d} kj} a^\dagger_{Z_j}. \tag{8}$$

### B. Bob's measurement

Bob's measurement apparatus is schematized in Fig. 1. For concreteness, here we describe the scenario where Bob's $Z$-basis detector measures the time of arrival of Alice's pulses. Nevertheless, the protocol and its proof are general and can be applied to other scenarios where Alice and Bob use different photonic degrees of freedom.

The TBS splits the signal received by Bob into a transmitted mode and a reflected mode. The reflected mode is measured by Bob's $Z$-basis detector, whose outcomes form Bob's raw key. The $Z$-basis detector is characterized by a mode-independent, or nominal, detector efficiency $\eta_Z$, which includes the insertion loss of the TBS. We indicate with $\mathcal{Z}$ the total time window in which the detector may click in a single measurement round. The time window $\mathcal{Z}$

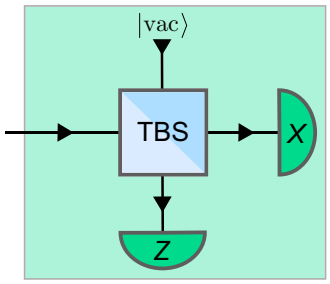


FIG. 1. Bob's measurement apparatus. The incoming signal (entering Bob's laboratory from the left) is split into two modes by a TBS. The transmitted mode is measured by an $X$-basis detector and the reflected mode is measured by by a $Z$-basis detector. The clicks in the $Z$-basis detector are used to generate key bits, while the joint detection statistics from both detectors are used for testing.

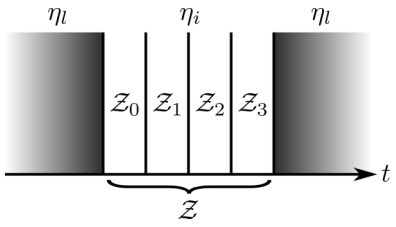


FIG. 2. Schematic representation of one measurement round. Only during the time interval $\mathcal{Z} = \bigcup_{j=0}^{d-1} \mathcal{Z}_j$ does the $Z$-basis detector register clicks and assign the corresponding outcome. The tunable beam splitter switches between transmittance $\eta_l$ outside the detection window $\mathcal{Z}$ and transmittance $\eta_i$ inside the detection window. This TBS setting is labeled by $(\eta_i, \eta_l)$. The statistics generated by different choices for $\eta_i$ and $\eta_l$ are used in the security proof to bound Eve's knowledge of the key.

is partitioned into discrete time bins $\mathcal{Z}_j$, with $\mathcal{Z} = \cup_{j=0}^{d-1} \mathcal{Z}_j$, that match those used by Alice to encode the key symbols. When a multiclick event occurs, i.e., a measurement with multiple clicks in different intervals $\mathcal{Z}_j$, Bob must map it to a single measurement outcome $j \in \{0, \ldots, d-1\}$ according to an arbitrary (potentially probabilistic) mapping; however, Bob cannot map it to the no-detection outcome $\emptyset$. The $Z$-basis detector could also be affected by dark counts. With $p_d^Z$ we indicate the probability that the $Z$-basis detector clicks in the interval $\mathcal{Z}_j$, for every $j$, given that no photon arrived in that interval.

The mode transmitted by the TBS is collected by Bob's $X$-basis detector, which can implement any measurement allowing Bob to discern the test symbols sent by Alice. The $X$-basis detector is characterized by a mode-independent, or nominal, detector efficiency $\eta_X$, which includes the TBS insertion loss and is assumed to be smaller than the efficiency of the key generation measurement, $\eta_X \leq \eta_Z$, otherwise the two measurements can be exchanged. Let $\mathcal{X}_k$ be the physical mode corresponding to the $k$th outcome and let $\mathcal{X} = \cup_{k=0}^{d-1} \mathcal{X}_k$ be the set of all modes that can cause a click in the $X$-basis detector. Similarly to for the $Z$-basis measurement, we assume that Bob maps each multiclick event to one of the $d$ measurement outcomes, $k \in \{0, \ldots, d-1\}$, excluding the no-detection outcome $\emptyset$, with an arbitrary mapping. Finally, we define $p_d^X$ to be the dark count probability in mode $\mathcal{X}_k$, for each $k$.

We allow the effective detection efficiency of the two measurement bases to arbitrarily differ due to, for example, tailored light modes that couple differently to the measurement apparatus of the two bases.

We now describe the capabilities of the TBS. The TBS can be tuned at high speed such that its transmittance can be set to different values within one measurement round. In particular, with $(\eta_i, \eta_l)$ we indicate a setting where the transmittance of the TBS, in one round, is set to $\eta_i$ within the duration of the time interval $\mathcal{Z}$ and to $\eta_l$ outside that interval. Note that the duration of each measurement round is typically longer than the time interval $\mathcal{Z}$ reserved for measuring in the key basis (due to, for example, a longer detection time required in the test basis). A graphical representation of a detection round and the corresponding TBS settings is given in Fig. 2. In our proof, we assume that the TBS cannot be influenced by eavesdroppers and, in particular, that its transmittance settings are mode independent.

Because of the TBS finite extinction ratio, we assume that the TBS transmittances are always contained in the range $[\eta_\downarrow, \eta_\uparrow] \subset [0, 1]$, where $\eta_\uparrow$ ($\eta_\downarrow$) represents the maximal (minimal) transmittance allowed by the TBS. The maximal and minimal transmittances need to satisfy the following two constraints, required by our security proof:

$$\eta_\uparrow > \frac{\eta_\downarrow}{1-\eta_\downarrow}, \tag{9}$$

$$\frac{\eta_X}{\eta_Z} > (\eta_\downarrow)^{-1} \left(1 - \sqrt{1 - \frac{\eta_\downarrow}{\eta_\uparrow}}\right). \tag{10}$$

We argue that the two constraints are not particularly stringent. For example, consider that, typically, the tuning of the TBS is symmetric such that $\eta_\downarrow = 1 - \eta_\uparrow$. Then the condition in Eq. (9) becomes: $\eta_\uparrow > (\sqrt{5}-1)/2 \approx 0.62$. This inequality is expected to be satisfied by TBSs that function as basis selectors. Similarly, the condition in Eq. (10), for $\eta_\downarrow = 1 - \eta_\uparrow$, can be satisfied, for example, with $\eta_X/\eta_Z \geq 0.6$ and $\eta_\uparrow > 0.87$, which should be achievable values. In particular, we observe that a high-speed TBS, as required by our proof and satisfying the constraints (9) and (10), could be experimentally implemented by, for example, a dual-output Mach-Zehnder modulator [40,41].

As a final remark, if Bob measures a photonic degree of freedom other than the arrival time in key generation

rounds, then $\mathcal{Z}$ would represent the set of modes that are detected by the $Z$-basis detector. Notably, the framework and the proof we provide are still applicable, as far as the TBS can be dynamically tuned along the new degree of freedom measured in the $Z$ basis.

In the following, we describe the generic QKD protocol, whose security is proven in Sec. IV.

**Protocol 1.** QKD protocol.

(1) The following describes one measurement round of the protocol, and it must be iterated for a sufficient number of rounds.

(a) Alice prepares a $Z$-basis state (event $T = Z$) with probability $p_Z$ and an $X$-basis state (event $T = X$) with probability $1 - p_Z$. When preparing a $Z$-basis ($X$-basis) state, Alice draws the symbol $j \in \{0, \ldots, d-1\}$ ($k \in \{0, \ldots, d-1\}$) uniformly at random and records the outcome in the random variable $Z_A$ ($X_A$). She then chooses an intensity $\mu_i \in \mathcal{S} := \{\mu_1, \mu_2, \mu_3\}$ with probabilities $p_{\mu_1}, p_{\mu_2}$, and $p_{\mu_3} = 1 - p_{\mu_1} - p_{\mu_2}$ and records it in a random variable $I_A$. On the basis of her choices, Alice prepares the phase-randomized coherent state $\rho_{Z_j}(\mu_i)$ ($\rho_{X_k}(\mu_i)$) given in Eq. (3) [Eq. (6)] and sends it to Bob via an insecure quantum channel. The states prepared by Alice in the two bases satisfy Eq. (7).

(b) In each round, Bob chooses one of seven different TBS settings, namely, $(\eta_i, \eta_\uparrow)$ for $i = 1, 2, 3$, $(\eta_i, \eta_\downarrow)$ for $i = 1, 2, 3$, and $(\eta_2, \eta_2)$. The transmittances are chosen as $\eta_1 = \eta_\uparrow$ and $\eta_3 = \eta_\downarrow$, and $\eta_2$ satisfies $\eta_\downarrow < \eta_2 < \eta_\uparrow$ [a close-to-optimal choice for maximizing the key rate is $\eta_2 = (1/4)(\sqrt{\eta_\downarrow} + \sqrt{\eta_\uparrow})^2$]. In particular, Bob chooses the setting $(\eta_\downarrow, \eta_\downarrow)$ with probability $p_Z$ or one of the other six settings with probability $(1 - p_Z)/6$ each.If the $Z$-basis detector ($X$-basis detector) clicks and returns outcome $j$ ($k$), Bob sets $Z_B = j$ ($X_B = k$). Otherwise, if the $Z$-basis detector ($X$-basis detector) does not click, Bob sets $Z_B = \emptyset$ ($X_B = \emptyset$).

(2) Public announcements: For each round, the parties announce the following information over an authenticated public channel. Alice announces the type of round she performed ($T$) and her intensity choice ($I_A$), while Bob announces the TBS setting and whether the $Z$-basis detector clicked ($Z_B \neq \emptyset$) or did not click ($Z_B = \emptyset$). The parties label the rounds where $T = Z$ and $Z_B \neq \emptyset$, and Bob selects the TBS setting $(\eta_\downarrow, \eta_\downarrow)$ as "key generation rounds," while the other rounds are labeled as "test rounds." For the test rounds, Bob additionally announces $X_B$ over the public channel.

(3) Gain estimation: From the information announced, the parties estimate the $Z$-basis gains:

$$G^{Z}_{\mu_j,(\eta_l,\eta_l)} = \Pr(Z_B \neq \emptyset | T = Z, I_A = \mu_j, (\eta_l, \eta_l)) \quad (11)$$

for each $\mu_j \in \mathcal{S}$ and $\eta_l \in \{\eta_\uparrow, \eta_2, \eta_\downarrow\}$. They also estimate the $X$-basis gains:

$$G^{X,\checkmark}_{\mu_j,(\eta_i,\eta_l)} = \Pr(X_B \neq \emptyset, Z_B \neq \emptyset | T = X, I_A = \mu_j, (\eta_i, \eta_l)), \quad (12)$$

$$G^{X,\emptyset}_{\mu_j,(\eta_i,\eta_l)} = \Pr(X_B \neq \emptyset, Z_B = \emptyset | T = X, I_A = \mu_j, (\eta_i, \eta_l)) \quad (13)$$

for $\mu_j \in \mathcal{S}$ and for $\eta_i \in \{\eta_\uparrow, \eta_2, \eta_\downarrow\}$ and $\eta_l \in \{\eta_\uparrow, \eta_\downarrow\}$.

(4) Error estimation: Bob reveals $Z_B$ for a subset of the key generation rounds in order for Alice to compute the QBER of the key generation rounds, for each intensity chosen by Alice:

$$Q_{Z,\mu_j} = \Pr(Z_A \neq Z_B | T = Z, I_A = \mu_j, (\eta_\downarrow, \eta_\downarrow), Z_B \neq \emptyset). \quad (14)$$

Alice also computes the QBERs of the test rounds with a detection in the $X$-basis detector ($X$-basis QBERs):

$$Q_{X,\mu_j,(\eta_i,\eta_\uparrow),\checkmark} = \Pr(X_A \neq X_B | T = X, I_A = \mu_j, (\eta_i, \eta_\uparrow), X_B \neq \emptyset, Z_B \neq \emptyset), \quad (15)$$

$$Q_{X,\mu_j,(\eta_i,\eta_\uparrow),\emptyset} = \Pr(X_A \neq X_B | T = X, I_A = \mu_j, (\eta_i, \eta_\uparrow), X_B \neq \emptyset, Z_B = \emptyset) \quad (16)$$

for $\eta_i \in \{\eta_\uparrow, \eta_2, \eta_\downarrow\}$ and $\mu_j \in \mathcal{S}$.

(5) Classical postprocessing: The parties, by performing error correction and privacy amplification, extract a shared secret key from the variables $Z_A$ (for Alice) and $Z_B$ (for Bob) relative to the key generation rounds where Bob did not reveal $Z_B$. The fraction of shared secret key bits established per protocol round, in the asymptotic limit of infinitely many rounds, is given by

$$\begin{aligned} r_\infty = & p_Z^2 \sum_{j=1}^{3} p_{\mu_j} \Big\{ e^{-\mu_j} \underline{Y^Z_{0,(\eta_\downarrow,\eta_\downarrow)}} \log_2 d \\ & + e^{-\mu_j} \mu_j \underline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}} \left[ \log_2 \left( \frac{1}{c} \right) - u(\overline{\tilde{e}_{X,1}}) \right] \\ & - G^Z_{\mu_j,(\eta_\downarrow,\eta_\downarrow)} u(Q_{Z,\mu_j}) \Big\}, \end{aligned} \quad (17)$$

and is called the "asymptotic key rate" of the protocol. Below we define the quantities appearing in the key rate expression.

We define the compatibility coefficient $c$ of Alice's states in the one-photon subspace [8]:

$$c = \max_{0\leq j,k\leq d-1} \left|\langle 1_{Z_j}| S^{-1} |1_{X_k}\rangle\right|^2, \tag{18}$$

where $S^{-1}$ is the generalized inverse of $S$ (the inverse on its support), with $S$ given in Eq. (7). The key rate is maximal when the compatibility coefficient is minimal (i.e., $c = 1/d$), and this occurs if Alice's states, in the one-photon subspace, form two mutually unbiased sets (the proof is given in Remark C1 in Appendix C):

$$\left|\langle 1_{Z_j}|1_{X_k}\rangle\right|^2 = \frac{1}{d} \text{ for all } j,k. \tag{19}$$

In turn, the condition in Eq. (19) can be obtained, for example, by combining the discrete Fourier transform (8) with the orthogonality of the states in one basis ($\langle 1_{Z_j}|1_{Z_{j'}}\rangle = \delta_{j,j'}$).

The function $u(x)$ appearing in Eq. (17) is defined as

$$u(x) = \begin{cases} h(x) + x\log_2(d-1) & \text{if } x \in \left(0, 1-\frac{1}{d}\right), \\ \log_2 d & \text{if } x \in \left[1-\frac{1}{d}, 1\right), \end{cases} \tag{20}$$

with $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ the binary entropy.

One of the main results of this paper is the derivation of the upper bound on the phase error rate of the protocol, $\overline{\tilde{e}_{X,1}}$. Because of its cumbersome expression, we report it in Appendix B as a function of (bounds on) the yields and test-round bit error rates.

Finally, $\underline{Y^Z_{n,(\eta_l,\eta_l)}}$ denotes a statistical lower bound on the $n$-photon yield in the $Z$ basis, i.e., the probability of a $Z$-basis detector click given that Alice sent $n$ photons and Bob chose the TBS setting $(\eta_l, \eta_l)$. The explicit expressions for $\underline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}$, $\underline{Y^Z_{0,(\eta_\downarrow,\eta_\downarrow)}}$, and of all the other bounds on the yields and bit error rates that appear in $\overline{\tilde{e}_{X,1}}$ are due to the decoy-state method and are reported in Appendix D.

For a complete overview of the notation and quantities defined in this paper, we refer the reader to Appendix A.

## IV. SECURITY PROOF

We analytically prove the asymptotic security of Protocol 1 under collective attacks by the eavesdropper, thereby deriving the key rate expression in Eq. (17). Security against coherent attacks cannot be directly inferred by one invoking de Finetti-type results (e.g., postselection technique [42,43]). Indeed, such results require a reduction to finite dimensions, which contrasts with the generality of our approach (Bob can receive states in an infinite number of different optical modes).

Unlike standard QKD security proofs [8–10], our proof does not rely on the assumption that the detection probability of the key generation measurement and of test measurement coincide for every input state. We allow Eve to add photons to Alice's single-photon pulses or prepare states in continuous degrees of freedom (e.g., time, frequency) [44,45], such that the detection probability of Eve's states depends on the measurement basis. Such attacks might not manifest themselves in asymmetric gains observed in an experiment, as Eve might be able to conceal her attack by acting symmetrically on both bases. Existing proofs [33–36] accounting for detection efficiency mismatches require, at the very least, that mode-dependent mismatches are fully characterized and known *a priori*.

The security proof presented here can avoid such a characterization by actively estimating the relevant quantities from the rich statistics generated with the TBS. More specifically, it uses the decoy-state method [37–39] to focus on the rounds where Alice sends exactly one photon. In parallel, it uses the TBS to apply the detector decoy technique [28] and estimate the photon number distribution of Bob's input states. Finally, it can estimate possible mode-dependent mismatches in the detection efficiency of the two measurement bases, thus not requiring their prior characterization.

In the following, we provide a simplified version of the security proof highlighting the steps that set it apart from previous proofs. The proof in full detail is reported in Appendix C.

*Proof.* According to the description of Protocol 1 in Sec. III, the parties extract the shared secret key from the rounds labeled as key generation rounds, where Alice sends a $Z$-basis state, Bob selects the TBS setting $(\eta_\downarrow, \eta_\downarrow)$, and the $Z$-basis detector clicks. We label the intersection of these three events with $\Omega_Z$. ■

The asymptotic secret key rate that can be extracted from the events $\Omega_Z$, under collective attacks, is lower-bounded by the Devetak-Winter (DW) rate [46]:

$$r \geq \Pr(\Omega_Z)\left[H(Z_A|I_AE)_{\rho|\Omega_Z} - H(Z_A|I_AZ_B)_{\rho|\Omega_Z}\right], \tag{21}$$

where $H(Z_A|I_AE)$ and $H(Z_A|I_AZ_B)$ are von Neumann entropies computed on the state shared by Alice, Bob, and Eve in a generic round, conditioned on the event $\Omega_Z$. This state is explicitly derived in Appendix C 1. Note that we can express

$$\Pr(\Omega_Z) = p_Z^2 \Pr(Z_B \neq \emptyset | T = Z, (\eta_\downarrow, \eta_\downarrow)). \tag{22}$$

The goal of the proof is to show that the key rate given in Eq. (17) is a lower bound of Eq. (21).

The second entropy in Eq. (21) quantifies Bob's uncertainty about Alice's key bit $Z_A$ and represents the information leakage of an optimal error correction scheme.

In Appendix C 2 we show how to bound this term with standard arguments in terms of the QBERs of the key generation rounds, Eq. (14), as follows:

$$H(Z_A|I_A Z_B)_{\rho|\Omega_Z} \leq \sum_{j=1}^{3} \frac{p_{\mu_j} G^Z_{\mu_j,(\eta_\downarrow,\eta_\downarrow)} u(Q_{Z,\mu_j})}{\Pr(Z_B \neq \emptyset | T = Z, (\eta_\downarrow, \eta_\downarrow))}, \tag{23}$$

where the function $u(x)$ is defined in Eq. (20) and the gain $G^Z_{\mu_j,(\eta_\downarrow,\eta_\downarrow)}$ is obtained as explained in step 3 of Protocol 1.

The remainder of the proof is devoted to deriving a lower bound on the first entropy in Eq. (21) in terms of observed statistics.

The first step consists in discarding the contributions to $H(Z_A|I_A E)_{\rho|\Omega_Z}$ relative to the rounds where Alice sends more than one photon to Bob. This is because such rounds are vulnerable to photon-number-splitting attacks [47] and hence cannot lead to shared secret bits. We show in Appendix C 3 a that the following inequality holds:

$$H(Z_A|I_A E)_{\rho|\Omega_Z} \geq \sum_{j=1}^{3} \frac{p_{\mu_j}}{\Pr(Z_B \neq \emptyset | T = Z, (\eta_\downarrow, \eta_\downarrow))} \left[ e^{-\mu_j} Y^Z_{0,(\eta_\downarrow,\eta_\downarrow)} \log_2 d + e^{-\mu_j} \mu_j Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)} H(Z_A|E)_{\rho|1,\Omega_Z} \right], \tag{24}$$

where $Y^Z_{n,(\eta_l,\eta_l)}$ is the $n$-photon $Z$-basis yield (see Appendix A), i.e., the probability that the $Z$-basis detector clicks, given that Alice sent $n$ photons encoded in a $Z$-basis state and Bob selected the TBS setting $(\eta_l, \eta_l)$, while $H(Z_A|E)_{\rho|1,\Omega_Z}$ is the entropy conditioned on a key generation round where Alice sent exactly one photon. Note that the conditional entropy is maximal when Alice sends the vacuum, $H(Z_A|E)_{\rho|0,\Omega_Z} = \log_2 d$, since Eve cannot be correlated to Alice's symbol when Alice sends the vacuum.

The next step, which is detailed in Appendix C 3 b, uses the uncertainty relation for von Neumann entropies [48–51] to derive a lower bound on the entropy $H(Z_A|E)_{\rho|1,\Omega_Z}$. In particular, thanks to the condition on Alice's states in the one-photon subspace (7), we can equivalently describe a key generation round in the entanglement-based picture. That is, there exists an entangled state $|\Psi_\tau\rangle_{AB}$, given by the purification of the state $\tau_B = S/d$ with $S$ in Eq. (7), and two fictitious measurements for Alice, called "Alice's $Z$-basis measurement" and "Alice's $X$-basis measurement" [8]. Then, Bob's conditional state, when Alice performs the $Z$-basis measurement ($X$-basis measurement) on system $A$ of $|\Psi_\tau\rangle_{AB}$ and obtains outcome $Z_A = j$ ($X_A = k$), coincides with the state $|1_{Z_j}\rangle$ ($|1_{X_k}\rangle$) sent to Bob in Protocol 1 when Alice draws the symbol $Z_A = j$ ($X_A = k$) and sends one photon [recall that Alice prepares probabilistic mixtures of Fock states with a Poissonian distribution, Eq. (3)].

We recall that the entropy $H(Z_A|E)_{\rho|1,\Omega_Z}$ is computed on the state of a key generation round, i.e., the state received by Bob and postselected on a detection by the $Z$-basis detector with TBS setting $(\eta_\downarrow, \eta_\downarrow)$. Hence, we update the state $|\Psi_\tau\rangle_{AB}$ to the following entangled state:

$$|\Psi\rangle = \left( \mathbb{1}_{AE} \otimes \frac{\sqrt{Z_\checkmark}}{\sqrt{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}} \right) (\mathbb{1}_A \otimes U_{BE}) |\Psi_\tau\rangle_{AB} \otimes |0\rangle_E, \tag{25}$$

where $U_{BE}$ is a unitary applied by Eve, jointly on Bob's system and Eve's system $E$, describing her collective attack, while $Z_\checkmark$ is the positive operator–valued measure (POVM) element corresponding to a detection of a key generation round, i.e., a detection by the $Z$-basis detector with TBS setting $(\eta_\downarrow, \eta_\downarrow)$. The denominator in the last expression ensures normalization. In this way, by applying the uncertainty relation on $|\Psi\rangle$ with Alice's two fictitious measurements, we obtain

$$H(Z_A|E)_{\rho|1,\Omega_Z} \geq \log_2 \frac{1}{c} - H(X_A|B)_\sigma, \tag{26}$$

where $c$ is given in Eq. (18) and where the entropy on the left-hand side is computed on the state $|\Psi\rangle$ after Alice's $Z$-basis measurement, which results in the entropy that needs to be bounded in Eq. (24). The entropy on the right-hand side is computed on the state $|\Psi\rangle$ after Alice's $X$-basis measurement, which reads

$$\sigma_{X_A B} = \frac{1}{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)} d} \sum_{k=0}^{d-1} |k\rangle\langle k|_{X_A} \otimes \sqrt{Z_\checkmark} \sigma_k \sqrt{Z_\checkmark}, \tag{27}$$

where $\sigma_k$ is the state received by Bob when Alice sends the one-photon $X$-basis state relative to symbol $X_A = k$:

$$\sigma_k = \mathrm{Tr}_E \left[ U_{BE} |1_{X_k}\rangle\langle 1_{X_k}|_B \otimes |0\rangle\langle 0|_E U^\dagger_{BE} \right]. \tag{28}$$

The state in Eq. (27) is properly normalized thanks to Eq. (7).

We can now focus on deriving an upper bound on the entropy $H(X_A|B)_\sigma$ appearing in Eq. (26). Since the entropy $H(X_A|B)_\sigma$ is conditioned on a quantum system, system $B$, we can apply a measurement map on system $B$ such that the resulting conditional Shannon entropy can be estimated with measurement statistics. To this aim, we first define Bob's test measurement by the POVM: $\{X_0, X_1, \ldots, X_{d-1}, X_\emptyset\}$, with $X_k$ the POVM element describing the detection of outcome $X_B = k$ by the $X$-basis detector, with TBS setting $(\eta_\uparrow, \eta_\uparrow)$. We can also define $X_\checkmark = \sum_{k=0}^{d-1} X_k$ to be the POVM element corresponding to a detection and $X_\emptyset = \mathbb{1} - X_\checkmark$ to be the POVM element corresponding to no detection. Then we consider the

measurement map

$$\mathcal{E}^{X}_{B\to\tilde{X}_B}(\cdot)=\sum_{k'=0}^{d-1}\mathrm{Tr}\left[\tilde{X}_{k'}\cdot\right]|k'\rangle\langle k'|_{\tilde{X}_B}, \tag{29}$$

where $\{\tilde{X}_{k'}\}_{k'=0}^{d-1}$ is a POVM defined from Bob's test measurement as follows:

$$\tilde{X}_k=(\sqrt{X_{\checkmark}})^{-1}X_k(\sqrt{X_{\checkmark}})^{-1}\oplus\frac{\mathbb{1}^{\perp}_{X_{\checkmark}}}{d}, \tag{30}$$

with $(\sqrt{X_{\checkmark}})^{-1}$ the inverse of $\sqrt{X_{\checkmark}}$ over its support and $\mathbb{1}^{\perp}_{X_{\checkmark}}$ the projector on the complement of the support of $X_{\checkmark}$. Then, by applying the measurement map (29) on system $B$ of Eq. (27), the following inequality holds [52]:

$$\begin{aligned}H(X_A|B)_{\sigma}&\leq H(X_A|\tilde{X}_B)_{\mathcal{E}^X(\sigma)}\\&\leq u(\tilde{e}_{X,1}),\end{aligned} \tag{31}$$

where in the second inequality we used Fano's inequality and defined the phase error rate

$$\tilde{e}_{X,1}=\sum_{k=0}^{d-1}\sum_{k'\neq k}\frac{\mathrm{Tr}\left[\tilde{X}_{k'}\sqrt{Z_{\checkmark}}\sigma_k\sqrt{Z_{\checkmark}}\right]}{Y^{Z}_{1,(\eta_{\downarrow},\eta_{\downarrow})}d}. \tag{32}$$

We can now lower-bound the Devetak-Winter rate in Eq. (21) by plugging in Eqs. (23) and (24), where we further bound the latter using Eq. (26) and subsequently Eq. (31). This leads to the following expression:

$$\begin{aligned}r\geq p_Z^2\textstyle\sum_{j=1}^{3}p_{\mu_j}\Big\{&e^{-\mu_j}\underline{Y^{Z}_{0,(\eta_{\downarrow},\eta_{\downarrow})}}\log_2 d\\&+e^{-\mu_j}\mu_j\underline{Y^{Z}_{1,(\eta_{\downarrow},\eta_{\downarrow})}}\left[\log_2\left(\frac{1}{c}\right)-u(\tilde{e}_{X,1})\right]\\&-G^{Z}_{\mu_j,(\eta_{\downarrow},\eta_{\downarrow})}u(Q_{Z,\mu_j})\Big\},\end{aligned} \tag{33}$$

where we used Eq. (22) to replace $\Pr(\Omega_Z)$ and replaced the $Z$-basis yields with their respective lower bounds, obtained with the decoy-state method [see Eqs. (D23) and (D28)].

The remainder of the proof is devoted to deriving a meaningful upper bound on the phase error rate, Eq. (32), in terms of the statistics collected in the test rounds. Indeed, the fact that $u(x)$ given in Eq. (20) is a monotonically non-decreasing function implies that the upper bound can be used to replace $\tilde{e}_{X,1}$ in Eq. (33) and obtain another lower bound on the DW rate.

In standard QKD security proofs [8,9] it is assumed that the detection probability of Bob's key generation measurement is equal to the detection probability of Bob's test measurement, for every input state. Mathematically, this amounts to an equality between the POVM elements corresponding to a detection in the two measurements:

$$Z_{\checkmark}=X_{\checkmark}. \tag{34}$$

By combining the assumption in Eq. (34) with Eq. (30), we find that the phase error rate reduces to the one-photon bit error rate of Bob's test measurement, as we derive explicitly in Appendix C 3 c:

$$\tilde{e}_{X,1}=\sum_{k=0}^{d-1}\sum_{k'\neq k}\frac{\mathrm{Tr}\left[X_{k'}\sigma_k\right]}{Y^{X}_{1,(\eta_{\uparrow},\eta_{\uparrow})}d}, \tag{35}$$

which can be readily estimated with the decoy-state method. The challenge in the more general setting addressed by this paper is to estimate the phase error rate when Eq. (34) is not assumed to hold.

### A. Phase error rate estimation

Here we briefly sketch the main ideas behind the estimation of the phase error rate. The full argument can be found in Appendix C 4, starting with a detailed overview of the main steps in Appendix C 4 a.

The first step in estimating the phase error rate in Eq. (32) consists in reducing the calculation to the subspace containing at most one photon in the set of modes $\mathcal{Z}$ detected by the $Z$-basis detector. We call this the "($\leq 1$)-subspace." The detailed description of this step is deferred to Appendixes C 4 b–C 4 e and C 4 j. Indeed, we expect most of the state $\bar{\sigma}$,

$$\bar{\sigma}=\sum_{k=0}^{d-1}\frac{\sigma_k}{d}, \tag{36}$$

which is the average state received by Bob when Alice sends one photon, to lie in the ($\leq 1$)-subspace in an honest implementation of the protocol [53]. The reduction to the ($\leq 1$)-subspace leads us to the following upper bound, reported in Eq. (C103):

$$\begin{aligned}\tilde{e}_{X,1}Y^{Z}_{1,(\eta_{\downarrow},\eta_{\downarrow})}\leq&\frac{\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}M_{\mathcal{Z}}^{\leq 1}\sum_{k'\neq k}X_{k'}M_{\mathcal{Z}}^{\leq 1}\right]}{p_d^{\mathcal{X}}+\eta_r\eta_{\uparrow}(1-p_d^{\mathcal{X}})}\\&+\frac{\eta_r\eta_{\uparrow}(1-p_d^{\mathcal{X}})}{p_d^{\mathcal{X}}+\eta_r\eta_{\uparrow}(1-p_d^{\mathcal{X}})}\mathrm{Tr}\left[\bar{\sigma}M_{\mathcal{Z}}^{\leq 1}\Pi^0_{\mathcal{X}}M_{\mathcal{Z}}^{\leq 1}\right]\\&+\overline{\Delta_2}+\overline{w}_{\mathcal{Z}}^{>1}.\end{aligned} \tag{37}$$

In the last expression, $\overline{w}_{\mathcal{Z}}^{>1}$ denotes an upper bound on the weight of the state $\bar{\sigma}$ outside the ($\leq 1$)-subspace,

$$\textstyle\sum_{\alpha=2}^{\infty}\mathrm{Tr}[\bar{\sigma}\,\Pi^{\alpha}_{\mathcal{Z}}]\leq\overline{w}_{\mathcal{Z}}^{>1}, \tag{38}$$

with $\Pi^{\alpha}_{\mathcal{Z}}$ being the projector onto the subspace containing $\alpha$ photons in the set of modes $\mathcal{Z}$. $\overline{\Delta_2}$ is a function of

both $\overline{w}_{\mathcal{Z}}^{>1}$ and $Y^{Z}_{1,(\eta_\downarrow,\eta_\downarrow)}$ and is derived in Eq. (C248). The operator $M_{\mathcal{Z}}^{\leq 1}$ is defined as

$$M_{\mathcal{Z}}^{\leq 1} = \sqrt{p_{\checkmark|0}}\Pi^0_{\mathcal{Z}} + \sqrt{p_{\checkmark|1}}\Pi^1_{\mathcal{Z}}, \tag{39}$$

where the probability $p_{\checkmark|\alpha}$ is defined in Eq. (C181). Similarly to $\Pi^{\alpha}_{\mathcal{Z}}$ for the $Z$-basis detector, we introduced the projector $\Pi^{\beta}_{\mathcal{X}}$ that projects on the subspace with $\beta$ photons in the set of modes $\mathcal{X}$. Finally, $\eta_r = \eta_X/\eta_Z$ is the ratio between the detector efficiencies of the two bases (by assumption $\eta_r \leq 1$) and $p_d^{\mathcal{X}}$ is the total probability of a dark count in the $X$-basis detector.

The remainder of the proof derives upper bounds on the first two terms on the right-hand side of Eq. (37) by using the detection statistics of the different TBS settings and by solving systems of linear equations. For the first term, the solution of a linear system yields the variables $\overline{\mathbb{E}}^{0}_{\eta_\uparrow}$, $\overline{\mathbb{E}}^{0,1}_{\eta_\uparrow}$, $\overline{\mathbb{E}}^{1t}_{\eta_\uparrow}$, and $\overline{\mathbb{E}}^{1r}_{\eta_\uparrow}$ and allows us to derive the following bound (see Appendixes C 4 f–C 4 j):

$$\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}M_{\mathcal{Z}}^{\leq 1}\sum_{k'\neq k}X_{k'}M_{\mathcal{Z}}^{\leq 1}\right] \leq p_{\checkmark|0}\overline{\mathbb{E}}^{0}_{\eta_\uparrow} + \sqrt{p_{\checkmark|0}p_{\checkmark|1}}\sqrt{\eta_\uparrow}\overline{\mathbb{E}}^{0,1}_{\eta_\uparrow} + p_{\checkmark|1}\left(\eta_\uparrow\overline{\mathbb{E}}^{1t}_{\eta_\uparrow} + (1-\eta_\uparrow)\overline{\mathbb{E}}^{1r}_{\eta_\uparrow}\right). \tag{40}$$

The second term in Eq. (37), in turn, is upper-bounded via

$$\mathrm{Tr}\left[\bar{\sigma}M_{\mathcal{Z}}^{\leq 1}\Pi^0_{\mathcal{X}}M_{\mathcal{Z}}^{\leq 1}\right] \leq p_{\checkmark|0}\overline{\left[w^0_{\mathcal{X}}\right]^0_{\mathcal{Z}}} + p_{\checkmark|1}\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}} + 2\sqrt{p_{\checkmark|0}p_{\checkmark|1}}\left(\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}\right)^{\frac{1}{2}}, \tag{41}$$

where the quantities $\overline{\left[w^0_{\mathcal{X}}\right]^0_{\mathcal{Z}}}$ and $\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}$ are derived with the detector decoy technique. The full derivation is reported in Appendixes C 4 k and C 4 l.

By inserting the bounds (40) and (41) into Eq. (37), we arrive at the final upper bound on the phase error rate, $\tilde{e}_{X,1} \leq \overline{\tilde{e}_{X,1}}$, where

$$\begin{aligned}\overline{\tilde{e}_{X,1}} = {} & \frac{1}{\underline{Y^{Z}_{1,(\eta_\downarrow,\eta_\downarrow)}}[p_d^{\mathcal{X}} + \eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})]}\left[p_{\checkmark|0}\overline{\mathbb{E}}^{0}_{\eta_\uparrow} + \sqrt{p_{\checkmark|0}p_{\checkmark|1}}\sqrt{\eta_\uparrow}\overline{\mathbb{E}}^{0,1}_{\eta_\uparrow} + p_{\checkmark|1}\left(\eta_\uparrow\overline{\mathbb{E}}^{1t}_{\eta_\uparrow} + (1-\eta_\uparrow)\overline{\mathbb{E}}^{1r}_{\eta_\uparrow}\right)\right] \\ & + \frac{\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}{\underline{Y^{Z}_{1,(\eta_\downarrow,\eta_\downarrow)}}[p_d^{\mathcal{X}} + \eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})]}\left[p_{\checkmark|0}\overline{\left[w^0_{\mathcal{X}}\right]^0_{\mathcal{Z}}} + 2\sqrt{p_{\checkmark|0}p_{\checkmark|1}}\left(\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}\right)^{\frac{1}{2}} + p_{\checkmark|1}\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}\right] \\ & + \frac{1}{\underline{Y^{Z}_{1,(\eta_\downarrow,\eta_\downarrow)}}}\left(\overline{\Delta_2} + \overline{w}_{\mathcal{Z}}^{>1}\right).\end{aligned} \tag{42}$$

Each quantity in the last expression is either known or directly expressed in terms of observed statistics via the relations given in Appendix B. In Appendix D, the formulas for the bounds on the yields are derived with the use of the decoy-state method.

By using the bound (42) in the key rate expression (33), we recover the asymptotic key rate of the protocol, Eq. (17), thus demonstrating that it is a lower bound of the DW rate in Eq. (21). This concludes the proof.

## V. SIMULATIONS

In this section we analyze the performance of our security proof on an experimental four-dimensional time-bin QKD protocol (Protocol 1), both in the case of an honest implementation (Sec. V A) and under an attack where Eve can partially control the detection probabilities of the two bases (Sec. V B). We benchmark the key rate resulting from our proof (17) with the asymptotic key rate of the standard decoy-BB84 protocol, with four outcomes per basis, which implicitly assumes basis-independent detection probabilities.

### A. High-dimensional time-bin QKD

We first consider an honest implementation of the protocol, without any attack in the quantum channel.

In the experimental setup in Refs. [29,30], Alice prepares $d = 4$ mutually orthogonal time bins for key generation, while the testing symbols are encoded in the relative phases between such pulses. In particular, if $a^{\dagger}_{Z_j}$ is the creation operator of one photon in the $j$ th time bin mode, the creation operators of the testing modes are given by the discrete Fourier transform of the time bin modes (8), such that the condition in Eq. (7) is satisfied and the compatibility coefficient of Alice's states is $c = 1/4$. Alice prepares the

pulses in both bases as phase-randomized coherent states, given by Eq. (3) for the $Z$ basis and Eq. (6) for the $X$ basis, with intensities $\mu_1$, $\mu_2 = 2\mu_3$, and $\mu_3 = 10^{-6}$ (note that weak decoy intensities are optimal). In the asymptotic limit, the optimal number of test rounds is negligible, and hence we set $p_Z = 1$ and $p_{\mu_1} = 1$.

Bob's measurement apparatus is described in Sec. III B, where the $Z$-basis measurement is realized with a single detector that detects the arrival time of the pulse, while the $X$-basis measurement is implemented by a dispersive medium followed by a time-of-arrival detection. From the arrival time of the dispersed signal, it is possible to infer the relative phases in the superposition of time bins sent by Alice in the test rounds. More details on Bob's $X$-basis measurement can be found in Refs. [29,30]. We set the largest and smallest transmittance allowed by the TBS to $\eta_\uparrow = 0.9$ and $\eta_\downarrow = 0.1$, respectively, such that Eq. (9) is satisfied. We also fix $\eta_2 = (1/4)(\sqrt{\eta_\downarrow} + \sqrt{\eta_\uparrow})^2 = 0.4$. We fix the insertion loss of the TBS and of the dispersive medium to 1 dB each, while the efficiency of the two detectors is 0.9. Thus, we have $\eta_Z = 0.9 \times 10^{-1/10}$ and $\eta_X = \eta_Z \times 10^{-1/10}$, such that Eq. (10) is satisfied. Finally, the dark count probability of the $Z$-basis detector ($X$-basis detector) in the whole detection window is $p_d^{\mathcal{Z}} = 10^{-4}$ ($p_d^{\mathcal{X}} = 1.2 \times 10^{-4}$, due to a longer detection window).

We adopt a simple channel model where Alice's pulses go through a bosonic channel with transmittance $\eta$, such that the pulses arriving at Bob are completely contained in the detection window $\mathcal{Z}$ used for key generation measurements (see Fig. 2). Moreover, we choose the duration of the detection window of the $X$-basis detector to be longer than in the $Z$ basis and long enough such that a negligible fraction of the dispersed signal (i.e., the signal exiting the dispersive medium) falls outside the detection window. We avoid modeling noise sources and instead assume that the signals arriving at Bob carry an intrinsic QBER $q_Z$ ($q_X$) in the $Z$ basis ($X$ basis). Therefore, the QBERs observed in the protocol, namely, $Q_{Z,\mu_j}$, $Q_{X,\mu_j,(\eta_i,\eta_\uparrow),\checkmark}$, and $Q_{X,\mu_j,(\eta_i,\eta_\uparrow),\emptyset}$, are the result of the intrinsic QBERs and of the dark counts in the detectors. We report the explicit formulas used for the gains and QBERs in Appendix E 1.

Using this channel model, in Fig. 3 we investigate the adaptability of our proof to different noise scenarios by computing the maximal tolerable channel loss, such that a positive secret key rate is obtained with Eq. (17) for various intrinsic QBERs $q_X$ and $q_Z$. We observe that our proof can tolerate up to 30 dB of loss and is resilient to noise, especially in the test basis. For example, for $q_Z = 2\%$ and 20 dB loss, we can extract a positive key rate for test-basis QBERs up to $q_X \approx 16\%$. By virtue of the considered honest implementation, different detection probabilities for the two bases are caused only by mode-independent asymmetries in the efficiencies and dark count probabilities of the two detectors ($\eta_Z \neq \eta_X$, $p_d^{\mathcal{Z}} \neq p_d^{\mathcal{X}}$). Still, they could be exploited by an attacker, as discussed in Sec. II. The key

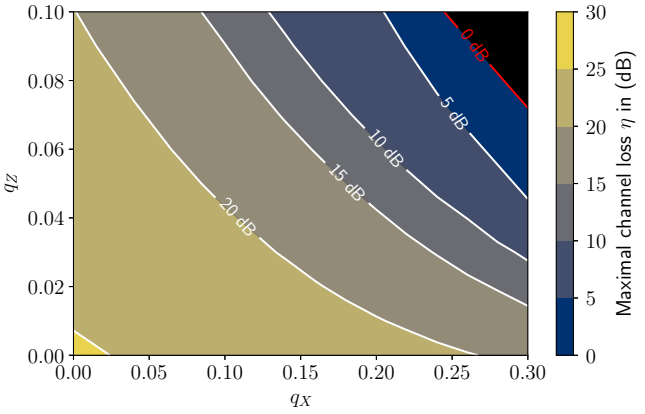


FIG. 3. Maximal tolerable channel loss for a positive key rate of a four-dimensional time-bin QKD protocol with nominal detection efficiency mismatch $\eta_X/\eta_Z = 10^{-1/10}$ for various channel-intrinsic QBERs $q_Z$ (key generation basis) and $q_X$ (test basis). The key rate is the one obtained from our proof, Eq. (17), and is optimized over the pulse intensity $\mu_1$. Furthermore, we fix the decoy intensities $\mu_2 = 2\mu_3 = 2 \times 10^{-6}$, the detectors' mode-independent efficiencies $\eta_Z = 0.9 \times 10^{-1/10}$ and $\eta_X = \eta_Z \times 10^{-1/10}$, the TBS parameters $\eta_\uparrow = 1 - \eta_\downarrow = 0.9$ and $\eta_2 = 0.4$, and the dark count probabilities $p_d^{\mathcal{X}} = 1.2\, p_d^{\mathcal{Z}} = 1.2 \times 10^{-4}$.

rate we provide in Eq. (17) allows for asymmetric detection probabilities and is secure even when the asymmetries are exploited or caused by an adversary. Conversely, the standard decoy-BB84 key rate for $d$-dimensional encoding [19],

$$r_{\text{decoy BB84}} = p_Z^2 \sum_{j=1}^{3} p_{\mu_j} \left\{ e^{-\mu_j} \underline{Y_0^Z} \log_2 d + e^{-\mu_j} \mu_j \underline{Y_1^Z} \left[ \log_2 d - u(\overline{e_{X,1}}) \right] - G_{\mu_j}^Z u(Q_{Z,\mu_j}) \right\}, \tag{43}$$

is derived under the assumption that the detection probability in the two bases coincides for every input state, i.e., that Eq. (34) holds. This effectively results in replacing the phase error rate upper bound in our rate, $\overline{\tilde{e}_{X,1}}$, with an upper bound on the bit error rate in the test basis, $\overline{e_{X,1}}$. However, the experimental setup considered [30] violates the assumption in Eq. (34) due to mode-independent (and potentially mode-dependent) asymmetries, implying that the decoy-BB84 key rate (43) cannot be applied to distill secure keys.

Nevertheless, in Fig. 4 we benchmark the performance of the key rate from our proof, Eq. (17), with the key rate in Eq. (43), where $d = 4$, for the honest implementation described above. Note that the TBS is not required by the security proof underlying Eq. (43). Hence, when computing the key rate via Eq. (43), we use only the TBS settings $(\eta_\uparrow, \eta_\uparrow)$ and $(\eta_\downarrow, \eta_\downarrow)$ to select the $X$ and $Z$ basis, respectively. The explicit expressions for the quantities appearing

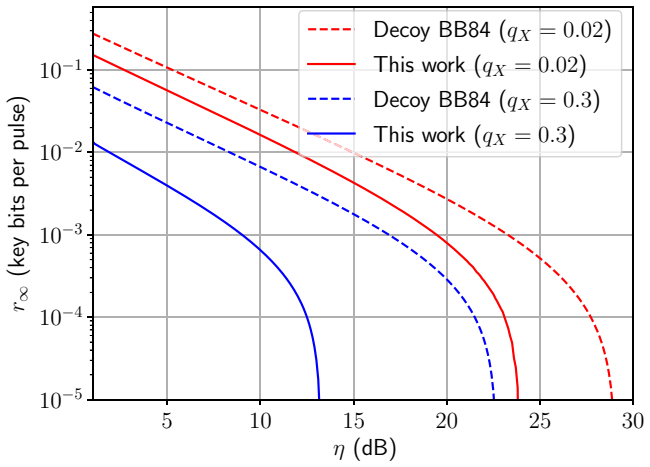


FIG. 4. Comparison of the secret key rate from our proof [Eq. (17), solid lines] with the decoy-BB84 key rate [Eq. (43), dashed lines] as a function of the channel loss $\eta$, for an honest implementation of a four-dimensional time-bin QKD protocol with nominal detection efficiency mismatch $\eta_X/\eta_Z = 10^{-1/10}$. We set $q_Z = 0.02$ and fix different values of the intrinsic test-basis QBER, $q_X$. All key rates are optimized over the intensity $\mu_1$. We further fix the decoy intensities $\mu_2 = 2\mu_3 = 2 \times 10^{-6}$, the detectors' mode-independent efficiencies $\eta_Z = 0.9 \times 10^{-1/10}$ and $\eta_X = \eta_Z \times 10^{-1/10}$, the TBS parameters $\eta_\uparrow = 1 - \eta_\downarrow = 0.9$ and $\eta_2 = 0.4$, and the dark count probabilities $p_d^Z = 10^{-4}$ and $p_d^X = 1.2 \times 10^{-4}$. In this honest implementation, the detection mismatch is mode independent and is caused only by different dark count rates and different nominal detection efficiencies for the two measurement bases. Even in this case, the decoy-BB84 key rate would not be applicable as it does not contemplate detection efficiency mismatches.

in Eq. (43) are reported in Appendix E 1. We observe that our key rate presents a gap to the decoy-BB84 key rate and that the gap widens for larger values of the QBER $q_X$.

### B. Attack-induced efficiency mismatch

We now consider an adversarial implementation of the four-dimensional time-bin QKD protocol (Protocol 1). Eve's attack could exploit one of the two vulnerabilities of the protocol, namely, the nominal detection efficiency mismatch between the two bases ($\eta_Z > \eta_X$) or a detection probability asymmetry induced by tailored light modes. An attack based on the first vulnerability was illustrated in Sec. II, and it involves adding photons to the one-photon signals sent from Alice. This would cause an increase of the gain of the lossier basis and could be noticed by Alice and Bob when compared with the gain in other runs where Eve is not present. Nevertheless, the standard decoy-BB84 key rate does not account for asymmetric nominal efficiencies, and hence the attack would be successful.

In this section, we consider the second vulnerability and devise an intercept-resend attack where the eavesdropper can actively control which basis clicks with tailored light pulses. In particular, in each round, with probability $w_Z$ ($w_X$), Eve replaces the quantum channel with an apparatus that intercepts Alice's pulse and measures it in the $Z$ basis ($X$ basis), such that the measurement can perfectly distinguish Alice's states when Alice's and Eve's bases coincide. Then, Eve prepares a highly localized one-photon pulse in the time domain (frequency domain), with width parametrized by $s$ ($\sigma$), which corresponds to the outcome she observed, and sends it through a quantum channel with transmittance $\xi_Z$ ($\xi_X$) to Bob. If Bob measures the pulse with the same basis as Eve, his outcome is almost perfectly correlated with Eve's. Otherwise, when Bob measures in the opposite basis, the outcome is approximately uniformly random and the detection probability is reduced. For example, if Eve intercepts the signal in the $Z$ basis and Bob measures it in the $X$ basis, her time-localized pulse would be stretched by the dispersive medium over a large time interval such that only a fraction of the outgoing pulse is contained in the detection window of the $X$-basis detector, thereby decreasing the detection probability in the $X$ basis. Moreover, the portion of the stretched signal within the detection window of the $X$-basis detector is nearly constant in amplitude, such that every outcome is approximately equally likely. When Eve does not perform the attack, we adopt the channel model from Sec. V A, where Alice and Bob are linked by a channel with transmittance $\eta$ and intrinsic QBERs given by $q_Z = q_X = 0.05$ (these values are chosen for comparison purposes and do not reflect currently experimentally achievable values). In Appendix E 2 we detail Eve's attack and the corresponding statistics observed by Alice and Bob.

To investigate the performance of our proof under the described attack, we assume that Alice is equipped with a deterministic single-photon source (note that this assumption is also made, for example, in Ref. [36]). Therefore, the decoy-state method becomes superfluous, and the key rate of Protocol 1 in Eq. (17) simplifies to the following expression (for $c = 1/d$):

$$r_{\text{no decoy}} = p_Z^2 Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)} \left[\log_2 d - u(\overline{\tilde{e}_{X,1}}) - u(e_{Z,1,(\eta_\downarrow,\eta_\downarrow)})\right], \tag{44}$$

where the one-photon yield $Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}$ and the one-photon error rate in the $Z$ basis $e_{Z,1,(\eta_\downarrow,\eta_\downarrow)}$ are directly observed quantities, replacing the corresponding gains and QBERs. By our removing the decoy-state method, the upper bound on the phase error rate $\overline{\tilde{e}_{X,1}}$ reduces to a simpler expression, as discussed in Appendix E 2. Similarly, when we assume there is a deterministic single-photon source, the decoy-BB84 protocol reduces to the original BB84 protocol, with key rate given by

$$r_{\text{BB84}} = p_Z^2 Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)} \left[\log_2 d - u(e_{X,1,(\eta_\uparrow,\eta_\uparrow)}) - u(e_{Z,1,(\eta_\downarrow,\eta_\downarrow)})\right], \tag{45}$$

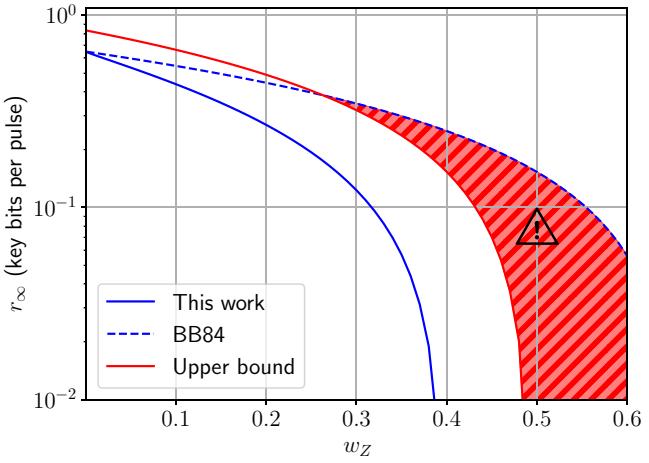


FIG. 5. Comparison of the secret key rate derived in this work [Eq. (44), solid blue line] with the BB84 key rate [Eq. (45), dashed blue line] and with an upper bound on the achievable key rate [Eq. (E45), solid red line] as a function of the probability that Eve intercepts the signal and measures it in the $Z$ basis (the key basis). All key rates are obtained under the assumption of a deterministic single-photon source (no decoys). With this attack, Eve can partially steer which basis clicks in each round to match the basis she measured in. The result is that the BB84 key rate, which does not account for attack-induced detection efficiency mismatches, overestimates the fraction of secret bits and surpasses the upper bound on the secret key rate, while the key rate from our proof remains below it. The plot parameters are as follows: number of symbols $d = 4$, intrinsic QBERs in the channel without Eve $q_Z = q_X = 0.05$, detectors' mode-independent efficiencies $\eta_Z = 9/10 \times 10^{-1/10}$ and $\eta_X = 10^{-1/10}\eta_Z$, TBS settings $\eta_\uparrow = 1 - \eta_\downarrow = 0.9$ and $\eta_2 = 0.4$, dark count probabilities $p_d^{\mathcal{Z}} = 10^{-4}$ and $p_d^{\mathcal{X}} = 1.2 \times 10^{-4}$, and channel loss of 1 dB, $\eta = 10^{-1/10}$. We partition the detection window of $\Delta_t = 1.132$ ns in the $Z$ basis into four time bins of width $\Delta_j = 0.283$ ns. Likewise, $\Delta_f = 4 \times \Delta_k = 4 \times 0.340$ ns in the $X$ basis. The group delay dispersion coefficient $\Phi_2$ of the dispersive medium is fixed to 0.01275 ns$^2$. See Appendix E 2 b for how these parameters enter the key rates.

where the phase error rate bound is replaced by the observed one-photon error rate in the $X$ basis $e_{X,1,(\eta_\uparrow,\eta_\uparrow)}$.

In Fig. 5, we plot the key rates in Eqs. (44) and (45) as a function of the probability of attacking the key basis, $w_Z$. For each value of $w_Z$, we optimize the parameters of Eve's attack $(w_X, s, \sigma, \xi_Z, \xi_X)$ such that the statistics observed by Alice and Bob in the BB84 protocol remain approximately equal to those in the scenario without attack. The intention is that of concealing Eve's attack when the parties run the standard BB84 protocol. Additionally, we plot an upper bound on the secret key rate that Alice and Bob can extract (the full derivation is presented in Sec. E 2). This is obtained by subtracting from Alice's raw key the number of bits known to Eve, which come from the rounds where Eve correctly guesses Alice's basis and from public error correction information.

From Fig. 5, we observe that Eve's attack cannot be completely concealed from the BB84 protocol, as its key rate decreases for increasing $w_Z$. However, the BB84 key rate surpasses the upper bound on the extractable key rate starting from $w_Z \approx 0.27$, while our key rate remains well below it. This shows that the BB84 protocol cannot fully grasp the extent of the information gained by Eve, returning an overly optimistic and, crucially, insecure key rate.

## VI. DISCUSSION

In Fig. 4, we highlighted a gap between our key rate (17) and the decoy-BB84 key rate (43) for the honest implementation of a four-dimensional time-bin QKD protocol. The gap is related to differing nominal efficiencies for the two measurement bases, i.e., $\eta_r = \eta_X/\eta_Z < 1$, which could be exploited by an attacker. Intuitively, however, the key rate should not penalized by asymmetric nominal efficiencies, unless an attacker is actively exploiting the asymmetry, as illustrated in Sec. II. The attack would entail adding photons to the signal resent to Bob, which would result in an increase of the weight of the state received by Bob in the subspace with more than one photon in the $Z$-basis detection interval, $\overline{w}_{\mathcal{Z}}^{>1}$. This parameter is otherwise null in an honest implementation without flaws, since it refers to the subset of one-photon signals sent by Alice.

In Appendix E 3, we show that our key rate is indeed insensitive to $\eta_r$—and matches the decoy-BB84 key rate—for honest implementations with asymmetric nominal efficiencies provided that we impose $\overline{w}_{\mathcal{Z}}^{>1} = 0$. In other words, when we impose that $\overline{w}_{\mathcal{Z}}^{>1}$ matches its true value for honest implementations, our key rate confirms the intuition that asymmetric nominal efficiencies do not influence the resulting key rate. We emphasize that this conclusion could not have been drawn from the decoy-BB84 rate since it does not apply to scenarios with $\eta_r < 1$. Conversely, when using the estimation for $\overline{w}_{\mathcal{Z}}^{>1}$ derived in our proof [see Eq. (B5)], we observe that our key rate decreases as the asymmetry in the detection efficiency of the two bases increases ($\eta_r$ decreases), generating the gap to the decoy-BB84 key rate. Therefore, the gap in Fig. 4 can be attributed to a nontight estimation of the parameter $\overline{w}_{\mathcal{Z}}^{>1}$ with the bound (B5) and could be improved by deriving tighter bounds.

A strong indication of how to improve the bound on the parameter $\overline{w}_{\mathcal{Z}}^{>1}$ comes from Fig. 5, where we observe that our key rate matches the BB84 key rate for $w_Z = 0$, i.e., in an honest implementation where Alice uses a deterministic single-photon source. In such an implementation, the yields and one-photon error rates are directly observed quantities, rather than being estimated with the decoy-state method. One of consequences is that the formula (B5) for $\overline{w}_{\mathcal{Z}}^{>1}$ returns the true value, zero (see Appendix E 2), allowing our key rate to match the BB84 key rate. This

suggests that increasing the number of decoy intensities (we assumed two decoy intensities in Protocol 1) may improve the estimation of $\overline{w}_{\mathcal{Z}}^{\geq 1}$ and reduce the gap to the decoy-BB84 key rate for honest implementations.

We already remarked that the standard BB84 protocol is not applicable to scenarios with asymmetric detection efficiencies, regardless of their being nominal or induced by the adversary. However, for the honest implementation in Fig. 4, the decoy-BB84 key rate represents de facto the largest amount of key that can be securely extracted, by matching our key rate when setting $\overline{w}_{\mathcal{Z}}^{\geq 1} = 0$. This is not the case for the attack corresponding to Fig. 5. The BB84 rate overestimates the fraction of secret key bits that can be extracted, by surpassing the upper bound on the secret key rate. Remarkably, when Eve attacks in the key basis 50% of the time ($w_Z = 0.5$), the BB84 key rate certifies more than 10% of secret bits per pulse when in reality no secure key can be extracted. This is caused by the nature of the attack we designed, where Eve can increase the fraction of rounds where she learns the key bits (increasing $w_Z$) without proportionately increasing her footprint: the $X$-basis error rate remains approximately constant. This is achieved by Eve preparing highly time-localized pulses when attacking in the $Z$ basis ($s \approx 0.017\Delta_j$), such that their detection probability in the $X$ basis is about 4.6 times less likely than in the same basis as Eve's. From the optimization, we observe that also attacking in the $X$ basis, i.e., $w_X > 0$, benefits the concealing of Eve's attack. In this case, Bob's $Z$ basis clicks with a probability reduced by a factor of about 2.3 compared with the $X$ basis. The result is that the vast majority of Bob's $X$-basis detections are events where either Eve attacks in the same basis or does not attack, thereby keeping the $X$-basis error rate low.

Crucially, the augmented statistics enabled by the TBS allow our proof to detect Eve's actions and reduce the key rate accordingly. Indeed, our key rate never surpasses the key rate upper bound in Fig. 5 and, curiously, presents a similar scaling with respect to $w_Z$. In other words, our security solution is capable of reducing the extractable key rate in proportion to the extent of adversarial attacks inducing asymmetric detection efficiencies in a given protocol run. This feature sets our proof apart from previous security proofs dealing with mode-dependent detection efficiencies [33–36].

To be more specific, we focus on the proofs that, like ours, do not restrict Eve's actions and allow her to, for example, add photons to Alice's pulses and induce detection efficiency asymmetries with tailored light modes [35,36]. Since such proofs are not capable of discerning whether Eve is exploiting or not exploiting the vulnerabilities of the measurement apparatus, they require the prior characterization of the largest detection probability ratio that Eve could induce with specific light modes between two detectors (and potentially two bases); we label this quantity $\kappa$. The key rates provided in Refs. [35,36] present a penalty depending on the value of $\kappa$, regardless of whether Eve is present or not. From the simulations reported in Refs. [35,36], we deduce that for a BB84 protocol with a deterministic single-photon source, 3 dB loss, and QBERs around 5%, no key can be extracted for $\kappa \geq 2$, even if Eve is not present. By using the same parameters ($\eta = 10^{-3/10}$, $q_Z = q_X = 0.05$, and $d = 2$) in the adversarial implementation studied in Sec. V B, our proof certifies 0.137 secret key bits per pulse when Eve is not present ($w_Z = 0$), which is also the rate obtained by naively applying the BB84 protocol. Only when Eve attacks the channel ($w_Z > 0$) and generates asymmetries in the detection probabilities of the two bases up to $\kappa = 4.6$ does our key rate decrease. We conclude that our proof is able to withstand larger mode-dependent asymmetries ($\kappa$) in the detection probabilities of vulnerable QKD setups compared with previous proposals. And, crucially, it delivers positive key rates when such vulnerabilities are not actively exploited by an eavesdropper.

## VII. CONCLUSION

We derived an analytical security proof for prepare-and-measure QKD protocols affected by basis-dependent detection probabilities. The proof can handle both nominal (mode-independent) and attack-induced (mode-dependent) detection efficiency mismatches. Compared with previous proposals, our proof requires no prior characterization of the efficiency mismatch generated by different light modes and it makes no assumption on the dimension of the states received by Bob. Moreover, the proof incorporates the decoy-state method and is capable of delivering positive key rates for QKD setups prone to large efficiency mismatches, such as the time-bin QKD protocol simulated in Sec. V. Our proof achieves this by actively monitoring the presence of attack-induced efficiency mismatches through a tunable beam splitter. As a result, it does not penalize the key rate unless an eavesdropper is actually attempting to control which basis clicks, whereas previous proofs always apply a penalty for the mere *possibility* of controlling the basis that clicks. In the most extreme case, where a QKD setup allows Eve to fully control which basis clicks, previous proofs cannot generate secret keys. Conversely, our proof will return positive key rates unless an adversary is actively exploiting the setup's flaws, in which case our key rate detects the attack and drops to zero. The merit for this remarkable feature is in part attributed to the tunable beam splitter, which we assume cannot be controlled by the adversary. Relaxing this assumption is an interesting direction for future work.

Further directions worth pursuing include extending our results to finite-key scenarios to apply our proof to real-world setups. Moreover, proving security against coherent attacks is desirable. Because of apparent difficulties in reducing our general model to finite dimensions, a possible

avenue is represented by an adaptation of the approach with entropic uncertainty relations for smooth entropies [8]. Nonetheless, we believe that the techniques introduced in this work can help address other security vulnerabilities of quantum cryptographic protocols.

*Note added.* While preparing the manuscript, we became aware of a related study [54]. That paper provides a security proof with finite-size effects for the decoy BB84 with mode-dependent detection efficiencies and active basis choice, going beyond the results in Ref. [36]. However, similarly to Ref. [36], the proof in Ref. [54] requires an *a priori* characterization of the detectors. Indeed, one of the required input parameters is the maximum relative difference in detection efficiencies that the eavesdropper can trigger. Conversely, in our proof no such parameter is required as it is estimated in real time during the execution of the QKD protocol.

## ACKNOWLEDGMENTS

F.G. contributed to this work exclusively on behalf of Heinrich-Heine-Universität Düsseldorf (previous affiliation). F.G. acknowledges funding from the Deutsche Forschungsgemeinschaft through Individual Grant No. BR2159/6-1. H.K., D.B., and N.Wy. acknowledge support by the QuantERA project QuICHE via the German Ministry of Education and Research (BMBF; Grant No. 16KIS1119K). D.B. and H.K. acknowledge support by the BMBF through the projects QuNET+ProQuake (Grant No. 16KISQ137) and QuKuK (Grant No. 16KIS1619). N.Wa. acknowledges funding from the BMBF (QPIC-1, Pho-Quant). M.K. and M.O. acknowledge the project QuICHE, supported by the National Science Centre, Poland (Project No. 2019/32/Z/ST2/00018) under QuantERA, which has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No. 731473. M.K., M.O., and A.W. acknowledge support by the Excellence Initiative—Research University of the University of Warsaw. G.C. and C.M. acknowledge the European Union's Horizon 2020 QuantERA ERA-NET Cofund in Quantum Technologies project QuICHE and support from the PNRR MUR project PE0000023-NQSTI. The authors thank Daniel Gauthier, Brian Smith, and Devashish Tupkary for insightful discussions.

## APPENDIX A: NOTATION

In Table I, we summarize the notation adopted throughout this paper.

## APPENDIX B: PHASE ERROR RATE BOUND

In this appendix we report, in a concise manner, the formulas that compose the upper bound on the phase error rate $\overline{\tilde{e}_{X,1}}$, which appears in the key rate of the protocol (17). For the notation and symbols used in the formulas below, see Appendix A.

The upper bound on the phase error rate is defined as follows:

$$\begin{aligned}\overline{\tilde{e}_{X,1}} = {} & \frac{1}{\underline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}[p_d^{\mathcal{X}} + \eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})]}\left[p_{\checkmark|0}\overline{\mathbb{E}}^0_{\eta_\uparrow} + \sqrt{p_{\checkmark|0}p_{\checkmark|1}}\sqrt{\eta_\uparrow}\overline{\mathbb{E}}^{0,1}_{\eta_\uparrow} + p_{\checkmark|1}\left(\eta_\uparrow\overline{\mathbb{E}}^{1t}_{\eta_\uparrow} + (1-\eta_\uparrow)\overline{\mathbb{E}}^{1r}_{\eta_\uparrow}\right)\right] \\ & + \frac{\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}{\underline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}[p_d^{\mathcal{X}} + \eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})]}\left[p_{\checkmark|0}\overline{\left[w^0_{\mathcal{X}}\right]^0_{\mathcal{Z}}} + 2\sqrt{p_{\checkmark|0}p_{\checkmark|1}}\left(\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}\right)^{\frac{1}{2}} + p_{\checkmark|1}\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}\right] + \frac{\overline{\Delta_2} + \overline{w}^{>1}_{\mathcal{Z}}}{\underline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}}. \end{aligned} \tag{B1}$$

The expression for $\overline{\tilde{e}_{X,1}}$ contains several quantities, which we now detail. We start by defining $p_{\checkmark|0} = p_d^{\mathcal{Z}}$ and $p_{\checkmark|1} = 1-(1-p_d^{\mathcal{Z}})\eta_\downarrow$, which are the probabilities that the $Z$-basis detector clicks, with TBS setting $(\eta_\downarrow,\eta_\downarrow)$, given that the state received by Bob contains zero photons or one photon, respectively, localized in $\mathcal{Z}$. We recall that

$$p_d^{\mathcal{Z}} = 1-(1-p_d^Z)^d, \tag{B2}$$

$$p_d^{\mathcal{X}} = 1-(1-p_d^X)^d \tag{B3}$$

are the total probability of a dark count in the $Z$-basis detector and the total probability of a dark count in the $X$-basis detector, respectively. We also define $\overline{\Delta_2}$ as

$$\overline{\Delta_2} = \sqrt{\left(\overline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}} - \min\left\{\overline{w}^{>1}_{\mathcal{Z}}, \frac{\overline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}}{2}\right\}\right)\min\left\{\overline{w}^{>1}_{\mathcal{Z}}, \frac{\overline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}}{2}\right\}}. \tag{B4}$$

TABLE I. Notation used in this paper. $W$ is a placeholder for the appropriate yield or error rate. The symbols ✓ and ∅ stand for a detection ($Z_B \neq \emptyset$) and no detection ($Z_B = \emptyset$) in Bob's $Z$-basis detector, respectively.

| Symbol | Name | Definition |
|---|---|---|
| $\mu_1, \mu_2, \mu_3$ | ⋯ | The three intensities used by Alice to prepare her states |
| $(\eta_i, \eta_l)$ | TBS setting | The transmittance of the TBS is set to $\eta_i$ in the interval $\mathcal{Z}$ and to $\eta_l$ otherwise |
| $\eta_\uparrow$ $(\eta_\downarrow)$ | ⋯ | Maximal (minimal) transmittance achievable by the TBS |
| $\eta_X$ | ⋯ | Detection efficiency of the $X$-basis detector, including the TBS insertion loss |
| $\eta_Z$ | ⋯ | Detection efficiency of the $Z$-basis detector, including the TBS insertion loss |
| $\eta_r$ | ⋯ | $\eta_r = \eta_X/\eta_Z$ |
| $\mathcal{X}$ | $X$-basis detection interval | The set of all modes detected by the $X$-basis detector: $\mathcal{X} = \cup_{k=0}^{d-1}\mathcal{X}_k$ |
| $\mathcal{Z}$ | $Z$-basis detection interval | The set of all modes detected by the $Z$-basis detector: $\mathcal{Z} = \cup_{j=0}^{d-1}\mathcal{Z}_j$ |
| $p_d^X$ | ⋯ | Probability of a dark count in mode $\mathcal{X}_k$ of the $X$-basis detector, for all $k$ |
| $p_d^Z$ | ⋯ | Probability of a dark count in mode $\mathcal{Z}_j$ of the $Z$-basis detector, for all $j$ |
| $p_d^{\mathcal{X}}$ $(p_d^{\mathcal{Z}})$ | ⋯ | Total probability of a dark count in the $X$-basis ($Z$-basis) detector if no photon is localized in $\mathcal{X}$ ($\mathcal{Z}$): $p_d^{\mathcal{X}} = 1-(1-p_d^Z)^d$ $(p_d^{\mathcal{Z}} = 1-(1-p_d^Z)^d)$ |
| $\overline{W}$ $(\underline{W})$ | ⋯ | Upper (lower) bound on $W$: $\overline{W} \geq W$ $(\underline{W} \leq W)$ |
| ⋯ | $(\leq 1)$-subspace | The subspace with at most one photon localized in $\mathcal{Z}$ |
| $[W]_{\mathcal{Z}}^{\leq 1}$ | ⋯ | $W$ is restricted to the $(\leq 1)$-subspace |
| $\tilde{e}_{X,1}$ | Phase error rate | The crucial parameter to be estimated in the security proof |
| $T$ | ⋯ | Random variable indicating whether Alice prepares a $Z$-basis state ($X$-basis state): $T = Z$ $(T = X)$ |
| $I_A$ | ⋯ | Alice's intensity choice in one round |
| $N_A$ | ⋯ | Number of photons sent by Alice in one round |
| $Z_A$ $(X_A)$ | ⋯ | Random variable storing Alice's symbol encoded in a $Z$-basis state ($X$-basis state) |
| $Z_B$ $(X_B)$ | ⋯ | Random variable storing the outcome of Bob's $Z$-basis detector ($X$-basis detector): $Z_B, X_B \in \{0, 1, \ldots, d-1, \emptyset\}$ |
| $G^Z_{\mu_j,(\eta_l,\eta_l)}$ | $Z$-basis gain | $G^Z_{\mu_j,(\eta_l,\eta_l)} = \Pr(Z_B \neq \emptyset \vert T = Z, I_A = \mu_j, (\eta_l, \eta_l))$ |
| $G^{X,\checkmark}_{\mu_j,(\eta_i,\eta_l)}$ | $X$-basis gain | $G^{X,\checkmark}_{\mu_j,(\eta_i,\eta_l)} = \Pr(X_B \neq \emptyset, Z_B \neq \emptyset \vert T = X, I_A = \mu_j, (\eta_i, \eta_l))$ |
| $G^{X,\emptyset}_{\mu_j,(\eta_i,\eta_l)}$ | $X$-basis gain | $G^{X,\emptyset}_{\mu_j,(\eta_i,\eta_l)} = \Pr(X_B \neq \emptyset, Z_B = \emptyset \vert T = X, I_A = \mu_j, (\eta_i, \eta_l))$ |
| $Q_{Z,\mu_j}$ | QBER of the key generation rounds | $Q_{Z,\mu_j} = \Pr(Z_A \neq Z_B \vert T = Z, I_A = \mu_j, (\eta_\downarrow, \eta_\downarrow), Z_B \neq \emptyset)$ |
| $Q_{X,\mu_j,(\eta_i,\eta_\uparrow),\checkmark}$ | $X$-basis QBER | $Q_{X,\mu_j,(\eta_i,\eta_\uparrow),\checkmark} = \Pr(X_A \neq X_B \vert T = X, I_A = \mu_j, (\eta_i, \eta_\uparrow), X_B \neq \emptyset, Z_B \neq \emptyset)$ |
| $Q_{X,\mu_j,(\eta_i,\eta_\uparrow),\emptyset}$ | $X$-basis QBER | $Q_{X,\mu_j,(\eta_i,\eta_\uparrow),\emptyset} = \Pr(X_A \neq X_B \vert T = X, I_A = \mu_j, (\eta_i, \eta_\uparrow), X_B \neq \emptyset, Z_B = \emptyset)$ |
| $Y^Z_{n,(\eta_l,\eta_l)}$ | $n$-photon $Z$-basis yield | $Y^Z_{n,(\eta_l,\eta_l)} = \Pr(Z_B \neq \emptyset \vert T = Z, N_A = n, (\eta_l, \eta_l))$ |
| $Y^{X,\checkmark}_{n,(\eta_i,\eta_l)}$ | $n$-photon $X$-basis yield ($n = 1$: test-round yield) | $Y^{X,\checkmark}_{n,(\eta_i,\eta_l)} = \Pr(X_B \neq \emptyset, Z_B \neq \emptyset \vert T = X, N_A = n, (\eta_i, \eta_l))$ |
| $Y^{X,\emptyset}_{n,(\eta_i,\eta_l)}$ | $n$-photon $X$-basis yield ($n = 1$: test-round yield) | $Y^{X,\emptyset}_{n,(\eta_i,\eta_l)} = \Pr(X_B \neq \emptyset, Z_B = \emptyset \vert T = X, N_A = n, (\eta_i, \eta_l))$ |
| $e_{X,n,(\eta_i,\eta_l),\checkmark}$ | $n$-photon $X$-basis bit error rate ($n = 1$: test-round bit error rate) | $e_{X,n,(\eta_i,\eta_l),\checkmark} = \Pr(X_A \neq X_B \vert T = X, N_A = n, (\eta_i, \eta_l), X_B \neq \emptyset, Z_B \neq \emptyset)$ |
| $e_{X,n,(\eta_i,\eta_l),\emptyset}$ | $n$-photon $X$-basis bit error rate ($n = 1$: test-round bit error rate) | $e_{X,n,(\eta_i,\eta_l),\emptyset} = \Pr(X_A \neq X_B \vert T = X, N_A = n, (\eta_i, \eta_l), X_B \neq \emptyset, Z_B = \emptyset)$ |
| $\Phi_2$ | Group delay dispersion coefficient | Group delay dispersion coefficient of the setup simulated in Fig. 5 |
| $\Delta_j$ $(\Delta_k)$ | Time-bin width | The widths of the time bins in Bob's time-of-arrival measurement for the $Z$ basis ($X$ basis), used to generate Fig. 5 |

We introduce an upper bound on the weight of the average state received by Bob (when Alice sends one photon) in the subspace with two or more photons localized in $\mathcal{Z}$:

$$\overline{w}_{\mathcal{Z}}^{>1} = \min\left\{1, \frac{\overline{(\eta_\uparrow-\eta_\downarrow)Y^{Z}_{1,(\eta_2,\eta_2)} - (1-\eta_2)(Y^{Z}_{1,(\eta_\downarrow,\eta_\downarrow)} - Y^{Z}_{1,(\eta_\uparrow,\eta_\uparrow)}) - (\eta_\uparrow-\eta_\downarrow)p_d^{\mathcal{Z}}}}{(1-p_d^{\mathcal{Z}})(\eta_\uparrow-\eta_\downarrow)(1-\eta_2)(1+\eta_2-\eta_\uparrow-\eta_\downarrow)}\right\}. \tag{B5}$$

Similarly, we report the following upper and lower bounds on the weight of the average state received by Bob, in the subspace with zero photons or one photon localized in $\mathcal{Z}$:

$$\overline{w}^0_{\mathcal{Z}} = \min\left\{1, \frac{\overline{\eta_\downarrow Y^{Z}_{1,(\eta_\uparrow,\eta_\uparrow)} - \eta_\uparrow(1-\eta_\uparrow)Y^{Z}_{1,(\eta_\downarrow,\eta_\downarrow)}} + \eta_\uparrow(1-\eta_\uparrow) - \eta_\downarrow + \eta_\uparrow^2\eta_\downarrow(1-p_d^{\mathcal{Z}})}{(1-p_d^{\mathcal{Z}})(1-\eta_\uparrow)\left[\eta_\uparrow - \eta_\downarrow(1+\eta_\uparrow)\right]}\right\}, \tag{B6}$$

$$\underline{w}^0_{\mathcal{Z}} = \max\left\{0, \frac{-\left(\overline{-\eta_\downarrow(1-\eta_\downarrow)Y^{Z}_{1,(\eta_\uparrow,\eta_\uparrow)} + \eta_\uparrow Y^{Z}_{1,(\eta_\downarrow,\eta_\downarrow)}}\right) + \eta_\uparrow - \eta_\downarrow(1-\eta_\downarrow) - \eta_\downarrow^2\eta_\uparrow(1-p_d^{\mathcal{Z}})}{(1-p_d^{\mathcal{Z}})(1-\eta_\downarrow)\left[\eta_\uparrow(1+\eta_\downarrow) - \eta_\downarrow\right]}\right\} \tag{B7}$$

and

$$\overline{w}^1_{\mathcal{Z}} = \min\left\{1, \frac{\overline{-(1-\eta_\downarrow^2)Y^{Z}_{1,(\eta_\uparrow,\eta_\uparrow)} + Y^{Z}_{1,(\eta_\downarrow,\eta_\downarrow)}} - \eta_\downarrow^2 p_d^{\mathcal{Z}}}{(1-p_d^{\mathcal{Z}})(1-\eta_\downarrow)\left[\eta_\uparrow(1+\eta_\downarrow) - \eta_\downarrow\right]}\right\}, \tag{B8}$$

$$\underline{w}^1_{\mathcal{Z}} = \max\left\{0, \frac{-\left(\overline{Y^{Z}_{1,(\eta_\uparrow,\eta_\uparrow)} - (1-\eta_\uparrow^2)Y^{Z}_{1,(\eta_\downarrow,\eta_\downarrow)}}\right) + \eta_\uparrow^2 p_d^{\mathcal{Z}}}{(1-p_d^{\mathcal{Z}})(1-\eta_\uparrow)\left[\eta_\uparrow - \eta_\downarrow(1+\eta_\uparrow)\right]}\right\}, \tag{B9}$$

respectively. These quantities appear in the upper bounds on the weight of the average state received by Bob in the subspace with zero photons in $\mathcal{X}$ and zero photons or one photon in $\mathcal{Z}$:

$$\overline{\left[w^0_{\mathcal{X}}\right]^0_{\mathcal{Z}}} = \min\left\{\overline{w}^0_{\mathcal{Z}}, \frac{(1-\eta_\uparrow\eta_r)\overline{\mathbb{Y}}^0_{\eta_\downarrow} - \eta_\downarrow\eta_r(1-\eta_\downarrow\eta_r)\underline{\mathbb{Y}}^0_{\eta_\uparrow} - \underline{w}^0_{\mathcal{Z}}p_d^{\mathcal{X}}(1-\eta_\uparrow\eta_r)(1-\eta_\downarrow\eta_r)^2}{\eta_\downarrow\eta_r(1-p_d^{\mathcal{X}})(2\eta_\uparrow\eta_r - 1 - \eta_r^2\eta_\uparrow\eta_\downarrow)} + \frac{\overline{w}^0_{\mathcal{Z}}}{1-p_d^{\mathcal{X}}}\right\} \tag{B10}$$

and

$$\begin{aligned}\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}} = \min\Bigg\{&\overline{w}^1_{\mathcal{Z}}, \frac{(1-\eta_\uparrow\eta_r)\left[\eta_\downarrow\overline{\mathbb{Y}}^{1t}_{\eta_\downarrow} + (1-\eta_\downarrow)\overline{\mathbb{Y}}^{1r}_{\eta_\downarrow}\right] - \eta_\downarrow\eta_r(1-\eta_\downarrow\eta_r)\left[\eta_\uparrow\underline{\mathbb{Y}}^{1t}_{\eta_\uparrow} + (1-\eta_\uparrow)\underline{\mathbb{Y}}^{1r}_{\eta_\uparrow}\right]}{\eta_\downarrow\eta_r(1-p_d^{\mathcal{X}})(2\eta_\uparrow\eta_r - 1 - \eta_r^2\eta_\uparrow\eta_\downarrow)} \\ &- \frac{\underline{w}^1_{\mathcal{Z}}p_d^{\mathcal{X}}(1-\eta_\uparrow\eta_r)(1-\eta_\downarrow\eta_r)^2}{\eta_\downarrow\eta_r(1-p_d^{\mathcal{X}})(2\eta_\uparrow\eta_r - 1 - \eta_r^2\eta_\uparrow\eta_\downarrow)} + \frac{\overline{w}^1_{\mathcal{Z}}}{1-p_d^{\mathcal{X}}}\Bigg\},\end{aligned} \tag{B11}$$

respectively. The bounds in Eqs. (B10) and (B11) contain bounds on the quantities $\mathbb{Y}^0_{\eta_l}$, $\mathbb{Y}^{1t}_{\eta_l}$, and $\mathbb{Y}^{1r}_{\eta_l}$. Such quantities are linked to the test-round yields as follows:

$$\begin{aligned}\overline{\mathbb{Y}}^0_{\eta_l} := \min\Bigg\{&\overline{w}^0_{\mathcal{Z}}, \frac{\sqrt{\eta_2\eta_\downarrow}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)(1-p_d^{\mathcal{Z}})}\overline{\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} \\ &- \frac{\sqrt{\eta_\uparrow\eta_\downarrow}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)(1-p_d^{\mathcal{Z}})}\underline{\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} \\ &+ \frac{\sqrt{\eta_\uparrow\eta_2}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)(1-p_d^{\mathcal{Z}})}\overline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}\Bigg\},\end{aligned} \tag{B12}$$

$$\underline{\mathbb{Y}}^{0}_{\eta_l} := \max\left\{0, \frac{\sqrt{\eta_2\eta_\downarrow}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\underline{\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} - \frac{\sqrt{\eta_\uparrow\eta_\downarrow}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\overline{\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} + \frac{\sqrt{\eta_\uparrow\eta_2}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\underline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}\right\} \tag{B13}$$

and

$$\overline{\mathbb{Y}}^{1t}_{\eta_l} := \min\left\{\overline{w}^{1}_{\mathcal{Z}}, \frac{\overline{\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)} - \frac{\underline{\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)} + \frac{\overline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\right\}, \tag{B14}$$

$$\overline{\mathbb{Y}}^{1r}_{\eta_l} := \min\left\{\overline{w}^{1}_{\mathcal{Z}}, \frac{1}{1-\eta_\downarrow}\overline{\left[Y^{X,\checkmark}_{1,(\eta_\downarrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} - \frac{p_d^{\mathcal{Z}}}{(1-\eta_\downarrow)(1-p_d^{\mathcal{Z}})}\underline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}\right\}, \tag{B15}$$

$$\underline{\mathbb{Y}}^{1t}_{\eta_l} := \max\left\{0, \frac{\underline{\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)} - \frac{\overline{\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)} + \frac{\underline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\right\}, \tag{B16}$$

$$\underline{\mathbb{Y}}^{1r}_{\eta_l} := \max\left\{0, \frac{1}{1-\eta_\downarrow}\underline{\left[Y^{X,\checkmark}_{1,(\eta_\downarrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} - \frac{p_d^{\mathcal{Z}}}{(1-\eta_\downarrow)(1-p_d^{\mathcal{Z}})}\overline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}\right\}. \tag{B17}$$

In particular, the bounds on the test-round yields restricted to the ($\leq 1$)-subspace read

$$\underline{\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} = \max\left\{0, \underline{Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}} - \sqrt{\overline{w}^{>1}_{\mathcal{Z}}} - \overline{w}^{>1}_{\mathcal{Z}}\right\}, \tag{B18}$$

$$\overline{\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} = \min\left\{1, \overline{Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}} + \sqrt{\overline{w}^{>1}_{\mathcal{Z}}}\right\}, \tag{B19}$$

$$\underline{\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} = \max\left\{0, \underline{Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}} - \sqrt{\overline{w}^{>1}_{\mathcal{Z}}} - \overline{w}^{>1}_{\mathcal{Z}}\right\}, \tag{B20}$$

$$\overline{\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} = \min\left\{1, \overline{Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}} + \sqrt{\overline{w}^{>1}_{\mathcal{Z}}}\right\}. \tag{B21}$$

We now report the expressions for the remaining quantities in Eq. (B1) that have not yet been defined, namely, $\overline{\mathbb{E}}^{0}_{\eta_\uparrow}, \overline{\mathbb{E}}^{0,1}_{\eta_\uparrow}, \overline{\mathbb{E}}^{1t}_{\eta_\uparrow}$, and $\overline{\mathbb{E}}^{1r}_{\eta_\uparrow}$. These are related to the products of the test-round yields and bit error rates as follows:

$$\overline{\mathbb{E}}^{0}_{\eta_\uparrow} := \min\left\{ \overline{w}^{0}_{\mathcal{Z}}, \frac{\sqrt{\eta_2\eta_\downarrow}\overline{\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_\uparrow)} e_{X,1,(\eta_\uparrow,\eta_\uparrow),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)} - \frac{\sqrt{\eta_\uparrow\eta_\downarrow}\underline{\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_\uparrow)} e_{X,1,(\eta_2,\eta_\uparrow),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)} \right.$$
$$\left. + \frac{\sqrt{\eta_\uparrow\eta_2}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\overline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_\uparrow)} e_{X,1,(\eta_\downarrow,\eta_\uparrow),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}} \right\}, \tag{B22}$$

$$\overline{\mathbb{E}}^{0,1}_{\eta_\uparrow} := \min\left\{ \frac{\overline{\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_\uparrow)} e_{X,1,(\eta_\uparrow,\eta_\uparrow),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}}{(1-p_d^{\mathcal{Z}})\sqrt{\eta_\uparrow}}, -\frac{(\sqrt{\eta_2}+\sqrt{\eta_\downarrow})\underline{\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_\uparrow)} e_{X,1,(\eta_\uparrow,\eta_\uparrow),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)} \right.$$
$$\left. + \frac{(\sqrt{\eta_\uparrow}+\sqrt{\eta_\downarrow})\overline{\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_\uparrow)} e_{X,1,(\eta_2,\eta_\uparrow),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)} - \frac{(\sqrt{\eta_\uparrow}+\sqrt{\eta_2})\underline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_\uparrow)} e_{X,1,(\eta_\downarrow,\eta_\uparrow),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)} \right\}, \tag{B23}$$

$$\overline{\mathbb{E}}^{1t}_{\eta_\uparrow} := \min\left\{ \overline{w}^{1}_{\mathcal{Z}}, \frac{\overline{\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_\uparrow)} e_{X,1,(\eta_\uparrow,\eta_\uparrow),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)} - \frac{\underline{\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_\uparrow)} e_{X,1,(\eta_2,\eta_\uparrow),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)} \right.$$
$$\left. + \frac{1}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\overline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_\uparrow)} e_{X,1,(\eta_\downarrow,\eta_\uparrow),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}} \right\}, \tag{B24}$$

$$\overline{\mathbb{E}}^{1r}_{\eta_\uparrow} := \min\left\{ \overline{w}^{1}_{\mathcal{Z}}, \frac{\overline{\left[Y^{X,\checkmark}_{1,(\eta_\downarrow,\eta_\uparrow)} e_{X,1,(\eta_\downarrow,\eta_\uparrow),\checkmark}\right]^{\leq 1}_{\mathcal{Z}}}}{1-\eta_\downarrow} - \frac{p_d^{\mathcal{Z}}}{(1-\eta_\downarrow)(1-p_d^{\mathcal{Z}})}\underline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_\uparrow)} e_{X,1,(\eta_\downarrow,\eta_\uparrow),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}} \right\}, \tag{B25}$$

where the bounds on the products of yields and error rates, restricted to the ($\leq 1$)-subspace, are given by

$$\underline{\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{\leq 1}_{\mathcal{Z}}} = \max\left\{0, \underline{Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}} - \sqrt{\overline{w}^{>1}_{\mathcal{Z}}} - \overline{w}^{>1}_{\mathcal{Z}}\right\}, \tag{B26}$$

$$\overline{\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{\leq 1}_{\mathcal{Z}}} = \min\left\{1, \overline{Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}} + \sqrt{\overline{w}^{>1}_{\mathcal{Z}}}\right\}, \tag{B27}$$

$$\underline{\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}} = \max\left\{0, \underline{Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}} - \sqrt{\overline{w}^{>1}_{\mathcal{Z}}} - \overline{w}^{>1}_{\mathcal{Z}}\right\}, \tag{B28}$$

$$\overline{\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}} = \min\left\{1, \overline{Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}} + \sqrt{\overline{w}^{>1}_{\mathcal{Z}}}\right\}. \tag{B29}$$

Finally, the upper and lower bounds on the yields and on the product of yields and bit error rates appearing in this appendix are obtained with the decoy-state method and are reported in Appendix D.

## APPENDIX C: SECURITY PROOF

In this appendix we prove the security of Protocol 1.

The DW bound [46] provides a lower bound on the asymptotic secret key rate of a QKD protocol subjected to collective attacks. According to the protocol's description, the shared secret key is extracted from the key generation rounds, i.e., the rounds where $T = Z$, the TBS is set to $(\eta_\downarrow, \eta_\downarrow)$, and $Z_B \neq \emptyset$. To keep the notation concise, we define the following intersections of events:

$$\Gamma_Z := [T = Z] \cap (\eta_\downarrow, \eta_\downarrow), \tag{C1}$$

$$\Omega_Z := \Gamma_Z \cap [Z_B \neq \emptyset]. \tag{C2}$$

The DW bound of our protocol then reads [55]

$$r \geq \Pr(\Omega_Z) \left[ H(Z_A|I_A E)_{\rho|\Omega_Z} - H(Z_A|I_A Z_B)_{\rho|\Omega_Z} \right], \tag{C3}$$

where $H(Z_A|I_A E)$ $[H(Z_A|I_A Z_B)]$ is the von Neumann entropy of Alice's key outcome $Z_A$ conditioned on Eve's (Bob's) total side information, while the subscript in the entropies indicates that they are computed on the state $\rho$ shared by Alice, Bob, and Eve, conditioned on the event $\Omega_Z$. Since Alice (Bob) chooses the setting $T = Z$ $[(\eta_\downarrow, \eta_\downarrow)]$ with probability $p_Z$, we have

$$\Pr(\Omega_Z) = p_Z^2 \Pr(Z_B \neq \emptyset|\Gamma_Z). \tag{C4}$$

The remainder of the proof consists in deriving appropriate bounds on the two entropies in Eq. (C3) to show that $r_\infty$, given in Eq. (17), is a lower bound on the DW rate (C3), hence proving the protocol's security.

### 1. Computing the postselected state

The first step is to obtain a mathematical expression for the quantum state $\rho_{Z_A I_A Z_B E|\Omega_Z}$ on which the two entropies in Eq. (C3) are computed.

To start with, we express the state of Alice's classical registers $(Z_A, I_A)$ and of Bob's $(B)$ and Eve's $(E)$ quantum systems in a $Z$-basis round as follows:

$$\begin{aligned}\rho_{Z_A I_A N_A B E} = &\sum_{j=0}^{d-1} \sum_{\mu_i \in \mathcal{S}} \frac{p_{\mu_i}}{d} |j\rangle\langle j|_{Z_A} \otimes |\mu_i\rangle\langle\mu_i|_{I_A} \\ &\otimes \sum_{n=0}^{\infty} \Pr(n|\mu_i) |n\rangle\langle n|_{N_A} \otimes U_{BE} |n_{Z_j}\rangle\langle n_{Z_j}|_B \\ &\otimes |0\rangle\langle 0|_E U_{BE}^\dagger. \end{aligned} \tag{C5}$$

Some comments are due. First, we added a classical register $N_A$, inaccessible to Alice, that contains the exact number of photons sent by Alice. Moreover, we modeled Eve's collective attack as a unitary acting on systems $BE$, which is not restrictive since we make no assumption on the dimension of Eve's quantum register $E$. Finally, the factor $1/d$ is due to the uniform probability with which Alice selects the symbol $Z_A$.

We mathematically describe Bob's measurement in terms of the following POVM:

$$\left\{ M_{j,k}^{(\eta_i,\eta_l)}, M_{j,\emptyset}^{(\eta_i,\eta_l)}, M_{\emptyset,k}^{(\eta_i,\eta_l)}, M_{\emptyset,\emptyset}^{(\eta_i,\eta_l)} \right\}, \tag{C6}$$

where the POVM element $M_{j,k}^{(\eta_i,\eta_l)}$ represents the outcome $Z_B = j, X_B = k$ when Bob selects $(\eta_i, \eta_l)$ as the TBS setting. Similarly, $M_{j,\emptyset}^{(\eta_i,\eta_l)}$ represents the outcome $Z_B = j$ and no click in the $X$-basis detector $(X_B = \emptyset)$ with TBS setting $(\eta_i, \eta_l)$. And so on for the others. From Eq. (C6), we can define a POVM that focuses on the outcomes of the $Z$-basis detector under the TBS setting $(\eta_\downarrow, \eta_\downarrow)$ and can be considered the effective POVM performed by Bob in the key generation rounds:

$$\{Z_0, Z_1, \ldots, Z_{d-1}, Z_\emptyset\}, \tag{C7}$$

with

$$Z_j = M_{j,\emptyset}^{(\eta_\downarrow,\eta_\downarrow)} + \sum_{k=0}^{d-1} M_{j,k}^{(\eta_\downarrow,\eta_\downarrow)}, \tag{C8}$$

$$Z_\emptyset = M_{\emptyset,\emptyset}^{(\eta_\downarrow,\eta_\downarrow)} + \sum_{k=0}^{d-1} M_{\emptyset,k}^{(\eta_\downarrow,\eta_\downarrow)}. \tag{C9}$$

For this, we call such a reduced measurement the "key generation measurement" of Bob. From Eq. (C7), in turn, we define the key generation measurement map $\mathcal{E}^Z_{B\to\tilde{B}Z_B}$. This map acts between the input system $B$ and two classical output systems, $Z_B$ and $\tilde{B}$, where $\tilde{B}$ is a classical register that contains coarse-grained information about the measurement outcome, namely, whether the detector clicked $(\tilde{B} = \checkmark)$ or did not click $(\tilde{B} = \emptyset)$. We thus have

$$\begin{aligned}\mathcal{E}^Z_{B\to\tilde{B}Z_B}(\cdot) = &\sum_{j=0}^{d-1} \mathrm{Tr}_B[Z_j \cdot\ ] |\checkmark\rangle\langle\checkmark|_{\tilde{B}} \otimes |j\rangle\langle j|_{Z_B} \\ &+ \mathrm{Tr}_B[Z_\emptyset \cdot\ ] |\emptyset\rangle\langle\emptyset|_{\tilde{B}} \otimes |\emptyset\rangle\langle\emptyset|_{Z_B}. \end{aligned} \tag{C10}$$

We now recast Bob's key generation measurement map as the concatenation of two quantum maps by following the formalism developed in Refs. [8,14]: $\mathcal{E}^Z_{B\to\tilde{B}Z_B} = \mathcal{E}^Z_{\tilde{B}B\to\tilde{B}Z_B} \circ \mathcal{E}^Z_{B\to\tilde{B}B}$. The first map that is applied can be viewed as a coarse-grained measurement:

$$\begin{aligned}\mathcal{E}^Z_{B\to\tilde{B}B}(\cdot) = &|\emptyset\rangle\langle\emptyset|_{\tilde{B}} \otimes \sqrt{Z_\emptyset} \cdot \sqrt{Z_\emptyset} + |\checkmark\rangle\langle\checkmark|_{\tilde{B}} \\ &\otimes \sqrt{Z_\checkmark} \cdot \sqrt{Z_\checkmark}, \end{aligned} \tag{C11}$$

where

$$Z_{\checkmark} = \sum_{j=0}^{d-1} Z_j. \tag{C12}$$

The second map replaces the coarse-grained outcomes of the first map with the actual outcomes of Bob's measurement and traces out the quantum system $B$. Let $\mathbb{1}_{Z_{\checkmark}}$ be the projector on the support of the operator $Z_{\checkmark}$. Then the second map reads

$$\begin{aligned}\mathcal{E}^{Z}_{\tilde{B}B\to\tilde{B}Z_B}(\cdot) = \sum_{j=0}^{d-1} |j\rangle\langle j|_{Z_B} \otimes \mathrm{Tr}_B\left[\left(|\checkmark\rangle\langle\checkmark|_{\tilde{B}} \otimes \tilde{Z}_j\right)\right. \\ \left.\cdot \left(|\checkmark\rangle\langle\checkmark|_{\tilde{B}} \otimes \mathbb{1}_B\right)\right] + |\emptyset\rangle\langle\emptyset|_{Z_B} \otimes |\emptyset\rangle\langle\emptyset|_{\tilde{B}} \\ \times \mathrm{Tr}_B[\,\cdot\,]\,|\emptyset\rangle\langle\emptyset|_{\tilde{B}},\end{aligned} \tag{C13}$$

where

$$\tilde{Z}_j = (\sqrt{Z_{\checkmark}})^{-1} Z_j (\sqrt{Z_{\checkmark}})^{-1} \oplus \frac{\mathbb{1}^{\perp}_{Z_{\checkmark}}}{d}, \tag{C14}$$

with $(\sqrt{Z_{\checkmark}})^{-1}$ the inverse of $\sqrt{Z_{\checkmark}}$ over its support, $\sqrt{Z_{\checkmark}}(\sqrt{Z_{\checkmark}})^{-1} = (\sqrt{Z_{\checkmark}})^{-1}\sqrt{Z_{\checkmark}} = \mathbb{1}_{Z_{\checkmark}}$, and with $\mathbb{1}^{\perp}_{Z_{\checkmark}}$ the projector on the complement of the support of $Z_{\checkmark}$. With the definition in Eq. (C14), both maps in Eqs. (C11) and (C13) are completely positive and trace preserving (CPTP) and their concatenation returns the original map (C10).

In a similar manner, from Eq. (C6) we can define a POVM that focuses on the outcomes of the $X$-basis detector, which would play the role of Bob's complementary measurement in a traditional QKD security proof:

$$\{X_0, X_1, \ldots, X_{d-1}, X_{\emptyset}\}, \tag{C15}$$

with

$$X_k = M^{(\eta_{\uparrow},\eta_{\uparrow})}_{\emptyset,k} + \sum_{j=0}^{d-1} M^{(\eta_{\uparrow},\eta_{\uparrow})}_{j,k}, \tag{C16}$$

$$X_{\emptyset} = M^{(\eta_{\uparrow},\eta_{\uparrow})}_{\emptyset,\emptyset} + \sum_{j=0}^{d-1} M^{(\eta_{\uparrow},\eta_{\uparrow})}_{j,\emptyset}. \tag{C17}$$

For this reason, we call this POVM the "test measurement" of Bob. We emphasize that the information gathered by the parties in the rounds labeled as test rounds exceeds what can be obtained by the above POVM, where the $Z$-basis detector outcomes are ignored and the TBS setting is fixed. Nevertheless, we are free to choose Bob's complementary measurement when defining the phase error rate, and our choice will be a POVM connected to Eq. (C15). The goal of the security proof will then be to show how the resulting phase error rate can be estimated from the full statistics observed in the test rounds.

We can thus define Bob's test measurement map as the quantum map implementing the POVM in Eq. (C15)

$$\begin{aligned}\mathcal{E}^{X}_{B\to\tilde{B}X_B}(\cdot) = \sum_{k=0}^{d-1} \mathrm{Tr}_B[X_k\ \cdot\ ]|\checkmark\rangle\langle\checkmark|_{\tilde{B}} \otimes |k\rangle\langle k|_{X_B} \\ + \mathrm{Tr}_B[X_{\emptyset}\ \cdot\ ]|\emptyset\rangle\langle\emptyset|_{\tilde{B}} \otimes |\emptyset\rangle\langle\emptyset|_{X_B},\end{aligned} \tag{C18}$$

and decompose it as the concatenation of two CPTP maps:

$$\mathcal{E}^{X}_{B\to\tilde{B}X_B} = \mathcal{E}^{X}_{\tilde{B}B\to\tilde{B}X_B} \circ \mathcal{E}^{X}_{B\to\tilde{B}B}, \tag{C19}$$

where the first map reads

$$\begin{aligned}\mathcal{E}^{X}_{B\to\tilde{B}B}(\cdot) = |\emptyset\rangle\langle\emptyset|_{\tilde{B}} \otimes \sqrt{X_{\emptyset}} \cdot \sqrt{X_{\emptyset}} + |\checkmark\rangle\langle\checkmark|_{\tilde{B}} \\ \otimes \sqrt{X_{\checkmark}} \cdot \sqrt{X_{\checkmark}},\end{aligned} \tag{C20}$$

with

$$X_{\checkmark} = \sum_{k=0}^{d-1} X_k, \tag{C21}$$

while the second map reads

$$\begin{aligned}\mathcal{E}^{X}_{\tilde{B}B\to\tilde{B}X_B}(\cdot) = \sum_{k=0}^{d-1} |k\rangle\langle k|_{X_B} \otimes \mathrm{Tr}_B\left[\left(|\checkmark\rangle\langle\checkmark|_{\tilde{B}} \otimes \tilde{X}_k\right)\right. \\ \left.\cdot \left(|\checkmark\rangle\langle\checkmark|_{\tilde{B}} \otimes \mathbb{1}_B\right)\right] \\ + |\emptyset\rangle\langle\emptyset|_{X_B} \otimes |\emptyset\rangle\langle\emptyset|_{\tilde{B}}\ \mathrm{Tr}_B[\,\cdot\,]\,|\emptyset\rangle\langle\emptyset|_{\tilde{B}},\end{aligned} \tag{C22}$$

where

$$\tilde{X}_k = (\sqrt{X_{\checkmark}})^{-1} X_k (\sqrt{X_{\checkmark}})^{-1} \oplus \frac{\mathbb{1}^{\perp}_{X_{\checkmark}}}{d}, \tag{C23}$$

with $(\sqrt{X_{\checkmark}})^{-1}$ the inverse of $\sqrt{X_{\checkmark}}$ over its support and $\mathbb{1}^{\perp}_{X_{\checkmark}}$ the projector on the complement of the support of $X_{\checkmark}$.

At this point, we can express the state of Alice's and Bob's classical registers $Z_A$ and $Z_B$ and Eve's quantum system $E$ in a $Z$-basis round where Bob selected the TBS setting $(\eta_{\downarrow}, \eta_{\downarrow})$ as follows:

$$\rho_{Z_A I_A N_A \tilde{B} Z_B E|\Gamma_Z} = \mathcal{E}^{Z}_{B\to\tilde{B}Z_B}\left(\rho_{Z_A I_A N_A BE}\right), \tag{C24}$$

where $\rho_{Z_A I_A N_A BE}$ is given in Eq. (C5) and where we used the definition of $\Gamma_Z$ in Eq. (C1). To obtain the state on which the entropies in Eq. (C3) are computed, we must postselect the state in Eq. (C24) on a detection in the $Z$-basis detector ($Z_B \neq \emptyset$). For this, we perform the projective measurement $\{|\emptyset\rangle\langle\emptyset|_{\tilde{B}}, |\checkmark\rangle\langle\checkmark|_{\tilde{B}}\}$ on system $\tilde{B}$ and select

the state conditioned on the outcome $\tilde{B} = \checkmark$ through the nonlinear map

$$\mathcal{P}(\cdot) = \frac{|\checkmark\rangle\langle\checkmark|_{\tilde{B}} \cdot |\checkmark\rangle\langle\checkmark|_{\tilde{B}}}{\mathrm{Tr}[\cdot\, |\checkmark\rangle\langle\checkmark|_{\tilde{B}}]} \tag{C25}$$

such that the state of a key generation round (i.e., conditioned on the event $\Omega_Z$) is given by [55]

$$\begin{aligned}\rho_{Z_A I_A N_A \tilde{B} Z_B E|\Omega_Z} &= \mathcal{P}\left(\rho_{Z_A I_A N_A \tilde{B} Z_B E|\Gamma_Z}\right) \\ &= \frac{\langle\checkmark|\rho_{Z_A I_A N_A \tilde{B} Z_B E|\Gamma_Z}|\checkmark\rangle_{\tilde{B}} \otimes |\checkmark\rangle\langle\checkmark|_{\tilde{B}}}{\Pr(Z_B \neq \emptyset|\Gamma_Z)},\end{aligned} \tag{C26}$$

where $\Pr(Z_B \neq \emptyset|\Gamma_Z) = \mathrm{Tr}[\rho_{Z_A I_A N_A \tilde{B} Z_B E|\Gamma_Z}|\checkmark\rangle\langle\checkmark|_{\tilde{B}}]$. The state in Eq. (C26) is the one needed to compute the entropies in Eq. (C3).

### 2. Computing the leakage

We first focus on the second entropy in Eq. (C3), which quantifies the optimal leakage due to error correction in the asymptotic regime and is computed on a reduced state of Eq. (C26), namely,

$$\rho_{Z_A I_A Z_B|\Omega_Z} = \frac{\langle\checkmark|\,\mathrm{Tr}_{N_A E}[\rho_{Z_A I_A N_A \tilde{B} Z_B E|\Gamma_Z}]|\checkmark\rangle_{\tilde{B}}}{\Pr(Z_B \neq \emptyset|\Gamma_Z)}. \tag{C27}$$

By explicitly calculating the above state through Eq. (C24), we obtain the expression

$$\begin{aligned}\rho_{Z_A I_A Z_B|\Omega_Z} = \sum_{\mu_i \in \mathcal{S}} &\frac{p_{\mu_i}}{\Pr(Z_B \neq \emptyset|\Gamma_Z)} |\mu_i\rangle\langle\mu_i|_{I_A} \\ &\otimes \sum_{j,j'=0}^{d-1} \frac{\mathrm{Tr}_B[Z_{j'} \zeta_{B|\mu_i,j}]}{d} |j\rangle\langle j|_{Z_A} \otimes |j'\rangle\langle j'|_{Z_B},\end{aligned} \tag{C28}$$

where $\zeta_{B|\mu_i,j}$ is the state received by Bob when Alice prepared the weak coherent pulse (WCP) with intensity $\mu_i$ encoding the symbol $Z_A = j$:

$$\zeta_{B|\mu_i,j} := \sum_{n=0}^{\infty} \Pr(n|\mu_i)\, \mathrm{Tr}_E[U_{BE}(|n_{Z_j}\rangle\langle n_{Z_j}| \otimes |0\rangle\langle 0|) U_{BE}^{\dagger}]. \tag{C29}$$

Hence, we recognize that $\mathrm{Tr}_B[Z_{j'} \zeta_{B|\mu_i,j}] = \Pr(Z_B = j'|\Gamma_Z, I_A = \mu_i, Z_A = j)$ is the probability that Bob obtains outcome $Z_B = j'$, given that Alice sent the symbol $Z_A = j$ encoded in a WCP of intensity $\mu_i$ and Bob chose the setting $(\eta_\downarrow, \eta_\downarrow)$. From this quantity we recover the $Z$-basis gain

$$\begin{aligned}G^Z_{\mu_i,(\eta_\downarrow,\eta_\downarrow)} &= \Pr(Z_B \neq \emptyset|\Gamma_Z, I_A = \mu_i) \\ &= \sum_{j,j'=0}^{d-1} \frac{\mathrm{Tr}_B[Z_{j'} \zeta_{B|\mu_i,j}]}{d},\end{aligned} \tag{C30}$$

and recast the state in Eq. (C28) as

$$\begin{aligned}\rho_{Z_A I_A Z_B|\Omega_Z} = &\sum_{\mu_i \in \mathcal{S}} \Pr(\mu_i|\Omega_Z) |\mu_i\rangle\langle\mu_i|_{I_A} \\ &\otimes \sum_{j,j'=0}^{d-1} \frac{\mathrm{Tr}_B[Z_{j'} \zeta_{B|\mu_i,j}]}{d G^Z_{\mu_i,(\eta_\downarrow,\eta_\downarrow)}} |j\rangle\langle j|_{Z_A} \otimes |j'\rangle\langle j'|_{Z_B},\end{aligned} \tag{C31}$$

where we used Bayes's rule and the definition of $\Omega_Z$ in Eq. (C2) to define

$$\Pr(\mu_i|\Omega_Z) = \frac{p_{\mu_i} G^Z_{\mu_i,(\eta_\downarrow,\eta_\downarrow)}}{\Pr(Z_B \neq \emptyset|\Gamma_Z)}. \tag{C32}$$

Then we observe that the state in Eq. (C31) is a classical-quantum state of the form $\sum_x p_x |x\rangle\langle x| \otimes \rho_x$ with $\rho_x$ normalized states, where the role of $x$ is played by $\mu_i$. Therefore, we can express its conditional entropy as

$$\begin{aligned}H(Z_A|I_A Z_B)_{\rho|\Omega_Z} &= \sum_{\mu_i \in \mathcal{S}} \Pr(\mu_i|\Omega_Z) H(Z_A|Z_B)_{\rho|\Omega_Z,\mu_i} \\ &\leq \sum_{\mu_i \in \mathcal{S}} \Pr(\mu_i|\Omega_Z)[h(Q_{Z,\mu_i}) \\ &\quad + Q_{Z,\mu_i} \log_2(d-1)] \\ &\leq \sum_{\mu_i \in \mathcal{S}} \frac{p_{\mu_i} G^Z_{\mu_i,(\eta_\downarrow,\eta_\downarrow)}}{\Pr(Z_B \neq \emptyset|\Gamma_Z)} u(Q_{Z,\mu_i}),\end{aligned} \tag{C33}$$

where we used Fano's inequality, with $Q_{Z,\mu_i}$ being the QBER of the key generation rounds where Alice used the intensity $\mu_i$, Eq. (14). In the last inequality we used Eq. (C32) and the definition of $u(x)$ in Eq. (20).

### 3. Lower-bounding Eve's uncertainty

#### *a. Discarding multiphoton contributions*

We now turn our attention to the first conditional entropy in Eq. (C3), representing Eve's uncertainty about Alice's key bit $Z_A$ in a key generation round. The goal is to obtain a lower bound that depends only on the statistics observed in the protocol. By the strong subadditivity, we can lower-bound the conditional entropy as follows:

$$H(Z_A|I_A E)_{\rho|\Omega_Z} \geq H(Z_A|I_A N_A E)_{\rho|\Omega_Z}, \tag{C34}$$

where the right-hand side describes Eve's uncertainty about $Z_A$ if Eve knew the exact photon number $N_A$ of the

signal sent by Alice. We now observe that the reduced state on which the conditional entropy is computed, which by definition (C26) reads

$$\rho_{Z_A I_A N_A E|\Omega_Z} = \mathrm{Tr}_{\tilde{B}Z_B}\left[\mathcal{P}\circ\mathcal{E}^Z_{\tilde{B}B\to\tilde{B}Z_B}\circ\mathcal{E}^Z_{B\to\tilde{B}B}\left(\rho_{Z_A I_A N_A BE}\right)\right], \tag{C35}$$

is equivalent to

$$\rho_{Z_A I_A N_A E|\Omega_Z} = \mathrm{Tr}_{B\tilde{B}}\left[\mathcal{P}\circ\mathcal{E}^Z_{B\to\tilde{B}B}\left(\rho_{Z_A I_A N_A BE}\right)\right]. \tag{C36}$$

In other words, the second part of Bob's key generation measurement map ($\mathcal{E}^Z_{\tilde{B}B\to\tilde{B}Z_B}$) has no effect on the reduced state required by the calculation of the conditional entropy in Eq. (C34). Since this state is conditioned on the event $\Omega_Z$ corresponding to a $Z$-basis detection without specifying the outcome, the coarse-grained measurement map ($\mathcal{E}^Z_{B\to\tilde{B}B}$) is enough to fix the state. By using Eq. (C5), we can express the state in Eq. (C36) as follows:

$$\begin{aligned}\rho_{Z_A I_A N_A E|\Omega_Z} = \frac{1}{\Pr(Z_B\neq\emptyset|\Gamma_Z)}\sum_{j=0}^{d-1}\sum_{\mu_i\in\mathcal{S}}\frac{p_{\mu_i}}{d}|j\rangle\langle j|_{Z_A}\\ \otimes|\mu_i\rangle\langle\mu_i|_{I_A}\otimes\sum_{n=0}^{\infty}\Pr(n|\mu_i)|n\rangle\langle n|_{N_A}\\ \otimes\Pr(Z_B\neq\emptyset|\Gamma_Z,N_A=n,Z_A=j)\,\phi_{E|n,j,\Omega_Z},\end{aligned} \tag{C37}$$

where we introduced the normalized state $\phi_{E|n,j,\Omega_Z}$ held by Eve in a key generation round, given that Alice sent the symbol $Z_B = j$ encoded in $n$ photons

$$\phi_{E|n,j,\Omega_Z} := \frac{\mathrm{Tr}_B\left[(\sqrt{Z_\checkmark}\otimes\mathbb{1}_E)U_{BE}|n_{Z_j}\rangle\langle n_{Z_j}|_B\otimes|0\rangle\langle 0|_E U^\dagger_{BE}(\sqrt{Z_\checkmark}\otimes\mathbb{1}_E)\right]}{\Pr(Z_B\neq\emptyset|\Gamma_Z,N_A=n,Z_A=j)}, \tag{C38}$$

and the probability

$$\begin{aligned}&\Pr(Z_B\neq\emptyset|\Gamma_Z,N_A=n,Z_A=j)\\ &\quad=\mathrm{Tr}\left[(Z_\checkmark\otimes\mathbb{1}_E)U_{BE}|n_{Z_j}\rangle\langle n_{Z_j}|_B\otimes|0\rangle\langle 0|_E U^\dagger_{BE}\right].\end{aligned} \tag{C39}$$

We can view the state in Eq. (C37) as a classical-quantum state between the systems $N_A$ and $Z_A I_A E$ by recasting it as follows:

$$\rho_{Z_A I_A N_A E|\Omega_Z} = \sum_{n=0}^{\infty}\Pr(n|\Omega_Z)|n\rangle\langle n|_{N_A}\otimes\rho_{Z_A I_A E|n,\Omega_Z}, \tag{C40}$$

where we defined the probability of Alice sending exactly $n$ photons, given a key generation round,

$$\Pr(n|\Omega_Z) = \frac{\sum_{\mu_i\in\mathcal{S}}p_{\mu_i}\Pr(n|\mu_i)\sum_{j=0}^{d-1}\Pr(Z_B\neq\emptyset|\Gamma_Z,N_A=n,Z_A=j)/d}{\Pr(Z_B\neq\emptyset|\Gamma_Z)}, \tag{C41}$$

and the normalized state

$$\rho_{Z_A I_A E|n,\Omega_Z} = \sum_{j=0}^{d-1}\frac{\Pr(Z_B\neq\emptyset|\Gamma_Z,N_A=n,Z_A=j)/d}{\Pr(Z_B\neq\emptyset|\Gamma_Z)\Pr(n|\Omega_Z)}|j\rangle\langle j|_{Z_A}\otimes\sum_{\mu_i\in\mathcal{S}}p_{\mu_i}\Pr(n|\mu_i)|\mu_i\rangle\langle\mu_i|_{I_A}\otimes\phi_{E|n,j,\Omega_Z}. \tag{C42}$$

Having expressed the state as a classical-quantum state in Eq. (C40), we can decompose its entropy as follows:

$$H(Z_A|I_A N_A E)_{\rho|\Omega_Z} = \sum_{n=0}^{\infty}\Pr(n|\Omega_Z)H(Z_A|I_A E)_{\rho|n,\Omega_Z}, \tag{C43}$$

where $H(Z_A|I_A E)_{\rho|n,\Omega_Z}$ is computed on the state (C42), which we recast as

$$\rho_{Z_A I_A E|n,\Omega_Z} = \rho_{I_A|n,\Omega_Z}\otimes\rho_{Z_A E|n,\Omega_Z}, \tag{C44}$$

where we defined the normalized states

$$\rho_{I_A|n,\Omega_Z} = \sum_{\mu_i\in\mathcal{S}} \frac{p_{\mu_i}\Pr(n|\mu_i)}{\Pr(n)} |\mu_i\rangle\langle\mu_i|_{I_A}, \tag{C45}$$

$$\begin{aligned}\rho_{Z_AE|n,\Omega_Z} &= \sum_{j=0}^{d-1} \frac{\Pr(n)\Pr(Z_B\neq\emptyset|\Gamma_Z,N_A=n,Z_A=j)/d}{\Pr(Z_B\neq\emptyset|\Gamma_Z)\Pr(n|\Omega_Z)} \\ &\quad\times |j\rangle\langle j|_{Z_A}\otimes\phi_{E|n,j,\Omega_Z} \\ &= \sum_{j=0}^{d-1} \frac{\Pr(Z_B\neq\emptyset|\Gamma_Z,N_A=n,Z_A=j)}{\sum_{l=0}^{d-1}\Pr(Z_B\neq\emptyset|\Gamma_Z,N_A=n,Z_A=l)} \\ &\quad\times |j\rangle\langle j|_{Z_A}\otimes\phi_{E|n,j,\Omega_Z},\end{aligned} \tag{C46}$$

where we used Eq. (C41) and

$$\Pr(n) = \sum_{\mu_i\in\mathcal{S}} p_{\mu_i}\Pr(n|\mu_i). \tag{C47}$$

From Eq. (C44) we observe that the state of $I_A$ is a tensor product with the state of $Z_AE$, which implies that

$$H(Z_A|I_AE)_{\rho|n,\Omega_Z} = H(Z_A|E)_{\rho|n,\Omega_Z}. \tag{C48}$$

By combining Eqs. (C43) and (C48), we obtain

$$H(Z_A|I_AN_AE)_{\rho|\Omega_Z} = \sum_{n=0}^{\infty}\Pr(n|\Omega_Z)H(Z_A|E)_{\rho|n,\Omega_Z}, \tag{C49}$$

where the entropy on the right-hand side is computed in Eq. (C46).

By combining Eqs. (C34) and (C49), we can lower bound the first entropy in Eq. (C3) as follows:

$$\begin{aligned}H(Z_A|I_AE)_{\rho|\Omega_Z} &\geq \sum_{n=0}^{\infty}\Pr(n|\Omega_Z)H(Z_A|E)_{\rho|n,\Omega_Z} \\ &= \sum_{n=0}^{\infty}\frac{Y^Z_{n,(\eta_\downarrow,\eta_\downarrow)}\Pr(n)}{\Pr(Z_B\neq\emptyset|\Gamma_Z)}H(Z_A|E)_{\rho|n,\Omega_Z},\end{aligned} \tag{C50}$$

where we used Eq. (C41) and defined the $n$-photon $Z$-basis yield as the detection probability of Bob's key generation measurement when Alice selects the $Z$ basis and sends $n$ photons as

$$\begin{aligned}Y^Z_{n,(\eta_\downarrow,\eta_\downarrow)} &:= \Pr(Z_B\neq\emptyset|\Gamma_Z,N_A=n) \\ &= \sum_{j=0}^{d-1}\Pr(Z_B\neq\emptyset|\Gamma_Z,N_A=n,Z_A=j)\frac{1}{d}.\end{aligned} \tag{C51}$$

Note that the yields are not directly observed and are instead estimated with the decoy-state method. Moreover, note that the yield in Eq. (C51) is well defined since $1/d = \Pr(Z_A=j) = \Pr(Z_A=j|N_A=n)$, where the last equality is because the distribution of the symbols and photons prepared by Alice is factorized: $\Pr(Z_A=j,N_A=n) = \Pr(Z_A=j)\Pr(N_A=n)$.

We can further lower-bound the entropy in Eq. (C50) by using the fact that $H(Z_A|E)_{\rho|n,\Omega_Z}\geq 0$ since $\rho_{Z_AE|n,\Omega_Z}$ is classical on $Z_A$. We obtain

$$\begin{aligned}H(Z_A|I_AE)_{\rho|\Omega_Z} &\geq \frac{Y^Z_{0,(\eta_\downarrow,\eta_\downarrow)}\Pr(0)}{\Pr(Z_B\neq\emptyset|\Gamma_Z)}H(Z_A|E)_{\rho|0,\Omega_Z} \\ &\quad+\frac{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}\Pr(1)}{\Pr(Z_B\neq\emptyset|\Gamma_Z)}H(Z_A|E)_{\rho|1,\Omega_Z},\end{aligned} \tag{C52}$$

where we discarded all the terms corresponding to events where Alice sends $n\geq 2$ photons. This is done because our ability to find a nontrivial lower bound on $H(Z_A|E)_{\sigma|n,\Omega_Z}$ for $n\geq 2$ is limited by the fact that we cannot apply the uncertainty relation on such entropies. Indeed, the states sent by Alice in key generation rounds and test rounds can be seen as originating from the same entangled state (which is a precondition for using the uncertainty relation) only at the single-photon level. In addition, in the event that $n\geq 2$, Eve can perform a photon-number-splitting attack and learn $Z_A$ while remaining undetected, which implies that $H(Z_A|E)_{\sigma|n,\Omega_Z}=0$ for $n\geq 2$.

We observe that the state $\rho_{Z_AE|0,\Omega_Z}$ in Eq. (C46) factorizes in the case that Alice sends the vacuum

$$\rho_{Z_AE|0,\Omega_Z} = \rho_{Z_A|0,\Omega_Z}\otimes\rho_{E|0,\Omega_Z}, \tag{C53}$$

because Eve's state (C38), $\phi_{E|0,j,\Omega_Z}$, is independent of $j$. This reflects the fact that Eve is uncorrelated with Alice's outcome $Z_A$ when Alice sends the vacuum. Therefore, we have

$$\begin{aligned}H(Z_A|E)_{\rho|0,\Omega_Z} &= H(Z_A)_{\rho|0,\Omega_Z} \\ &= H\left(\left\{\frac{\Pr(Z_B\neq\emptyset|\Gamma_Z,N_A=0,Z_A=j)}{\sum_{l=0}^{d-1}\Pr(Z_B\neq\emptyset|\Gamma_Z,N_A=0,Z_A=l)}\right\}_{j=0}^{d-1}\right),\end{aligned} \tag{C54}$$

where the entropy in the second line is the Shannon entropy of the enclosed distribution. From Eq. (C39) we observe that $\Pr(Z_B\neq\emptyset|\Gamma_Z,N_A=0,Z_A=j) = \Pr(Z_B\neq\emptyset|\Gamma_Z,N_A=0)$, i.e., the distribution is independent of the symbol $Z_A$ when Alice sends the vacuum. Thus, the distribution in the Shannon entropy simplifies to a uniform distribution of $d$ outcomes, and we obtain

$$H(Z_A|E)_{\rho|0,\Omega_Z} = \log_2 d. \tag{C55}$$

By using Eq. (C55) in Eq. (C52), we obtain

$$H(Z_A|I_AE)_{\rho|\Omega_Z} \geq \frac{Y^Z_{0,(\eta_\downarrow,\eta_\downarrow)}\Pr(0)}{\Pr(Z_B \neq \emptyset|\Gamma_Z)}\log_2 d + \frac{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}\Pr(1)}{\Pr(Z_B \neq \emptyset|\Gamma_Z)}H(Z_A|E)_{\rho|1,\Omega_Z}. \tag{C56}$$

### *b. Using uncertainty relations*

We are left to find a lower bound on the entropy $H(Z_A|E)_{\rho|1,\Omega_Z}$ of Alice's outcome $Z_A$ of a key generation round where she sends exactly one photon, conditioned on Eve's quantum side information. The entropy is computed on the state in Eq. (C46), which for $n = 1$ can be recast as

$$\rho_{Z_AE|1,\Omega_Z} = \sum_{j=0}^{d-1}\frac{1}{dY^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}|j\rangle\langle j|_{Z_A} \otimes \mathrm{Tr}_B\left[(\sqrt{Z_\checkmark}\otimes \mathbb{1}_E)U_{BE}|1_{Z_j}\rangle\langle 1_{Z_j}| \otimes |0\rangle\langle 0|_E U^\dagger_{BE}(\sqrt{Z_\checkmark}\otimes \mathbb{1}_E)\right], \tag{C57}$$

where we used Eqs. (C51) and (C38). The sought bound is obtained through the uncertainty relation for entropies with quantum side information, whose statement is reported below.

*Lemma 1 (entropic uncertainty relation [48–51]).* Let $\sigma_{ABE}$ be a normalized quantum state and let $\{M^Z_j\}_j$ and $\{M^X_k\}_k$ be two POVMs on $A$. It holds that

$$H(Z_A|E)_\sigma + H(X_A|B)_\sigma \geq \log_2 \frac{1}{\max_{j,k}\left\|\sqrt{M^Z_j}\sqrt{M^X_k}\right\|^2_\infty}, \tag{C58}$$

where the first entropy and the second entropy are computed on the classical-quantum states:

$$\sigma_{Z_AE} = \sum_j |j\rangle\langle j|_{Z_A}\otimes \mathrm{Tr}_{AB}\left[(M^Z_j\otimes \mathbb{1}_{BE})\sigma_{ABE}\right], \tag{C59}$$

$$\sigma_{X_AB} = \sum_k |k\rangle\langle k|_{X_A}\otimes \mathrm{Tr}_{AE}\left[(M^X_k\otimes \mathbb{1}_{BE})\sigma_{ABE}\right], \tag{C60}$$

respectively.

We choose an appropriate state $\sigma_{ABE}$ and POVMs on $A$ such that the first entropy in Eq. (C58) coincides with the entropy we need to bound in Eq. (C56). To this aim, we define the average state sent by Alice in any round, restricted to the single-photon subspace,

$$\tau := \frac{1}{d}\sum_{j=0}^{d-1}|1_{Z_j}\rangle\langle 1_{Z_j}| = \frac{1}{d}\sum_{k=0}^{d-1}|1_{X_k}\rangle\langle 1_{X_k}|, \tag{C61}$$

where the equality between the average state of $Z$-basis rounds and the average state of $X$-basis rounds is due to the assumption (7). We then define $\tau_{AB} = |\Psi_\tau\rangle\langle\Psi_\tau|$ to be the purification of $\tau$ and define the POVMs $\{M^Z_j\}_j$ and $\{M^X_k\}_k$ acting on the purifying system $A$:

$$M^Z_j = \frac{1}{d}\left(\tau^{-1/2}\right)^T\left(|1_{Z_j}\rangle\langle 1_{Z_j}|\right)^T\left(\tau^{-1/2}\right)^T, \tag{C62}$$

$$M^X_k = \frac{1}{d}\left(\tau^{-1/2}\right)^T\left(|1_{X_k}\rangle\langle 1_{X_k}|\right)^T\left(\tau^{-1/2}\right)^T, \tag{C63}$$

where the superscript "$T$" represents the transpose with respect to the Schmidt basis of $\tau_{AB}$. Then, according to Lemma 14 in Ref. [8], the reduced states on $B$, after application of the POVMs (C62) and (C63) on system $A$ of $\tau_{AB}$, are exactly the states Alice prepares in the one-photon subspace (multiplied by their probability):

$$\mathrm{Tr}_A\left[(M^Z_j\otimes \mathbb{1}_B)\tau_{AB}\right] = \frac{|1_{Z_j}\rangle\langle 1_{Z_j}|}{d}, \tag{C64}$$

$$\mathrm{Tr}_A\left[(M^X_k\otimes \mathbb{1}_B)\tau_{AB}\right] = \frac{|1_{X_k}\rangle\langle 1_{X_k}|}{d}. \tag{C65}$$

Moreover, Lemma 14 in Ref. [8] shows that

$$\max_{j,k}\left\|\sqrt{M^Z_j}\sqrt{M^X_k}\right\|^2_\infty = \max_{0\leq j,k\leq d-1}\left\||1_{Z_j}\rangle\langle 1_{Z_j}|S^{-1}|1_{X_k}\rangle\langle 1_{X_k}|\right\|^2_\infty = c \tag{C66}$$

for the above-defined POVMs, where $S$ is given in Eq. (7), $\|A\|_\infty$ is the largest singular value of $A$, and $c$ is given in Eq. (18).

*Remark 1.* As discussed in Sec. III, the protocol's key rate (17) is maximized when the compatibility coefficient $c$ is minimal: $c = 1/d$. Here we show that a sufficient condition to attain this is that Alice's one-photon states form two mutually unbiased sets:

$$\left|\langle 1_{Z_j}|1_{X_k}\rangle\right|^2 = \frac{1}{d}\ \text{for all}\ j,k. \tag{C67}$$

*Proof.* The proof hinges on the fact that when two sets of vectors, $\{|1_{Z_j}\rangle\}_j$ and $\{|1_{X_k}\rangle\}_k$, sum to the same operator $S$ by Eq. (7) and are mutually unbiased (C67), then they are orthogonal sets.

To see this, consider the scalar $\langle 1_{Z_j}|S|1_{Z_j}\rangle$. By virtue of $S=\sum_k |1_{X_k}\rangle\langle 1_{X_k}|$ and Eq. (C67), we get $\langle 1_{Z_j}|S|1_{Z_j}\rangle = 1$. At the same time, by using the other expression for $S$, we get $\langle 1_{Z_j}|S|1_{Z_j}\rangle = 1+\sum_{j'\neq j}\left|\langle 1_{Z_j}|1_{Z_{j'}}\rangle\right|^2$, which implies that $\sum_{j'\neq j}\left|\langle 1_{Z_j}|1_{Z_{j'}}\rangle\right|^2 = 0$. This implies that the set of vectors $\{|1_{Z_j}\rangle\}_j$ is orthonormal:

$$\left|\langle 1_{Z_j}|1_{Z_{j'}}\rangle\right|^2 = \delta_{j,j'}. \tag{C68}$$

Similarly for the set $\{|1_{X_k}\rangle\}_k$,

$$\left|\langle 1_{X_k}|1_{X_{k'}}\rangle\right|^2 = \delta_{k,k'}. \tag{C69}$$

Thus, we deduce that $S$ is the identity in the subspace defined by $\{|1_{Z_j}\rangle\}_j$ (or $\{|1_{X_k}\rangle\}_k$), which simplifies Eq. (18) as follows:

$$\begin{aligned} c &= \max_{0\le j,k\le d-1}\left|\langle 1_{Z_j}||1_{X_k}\rangle\right|^2 \\ &= \frac{1}{d}, \end{aligned} \tag{C70}$$

where in the second equality we used Eq. (C67). ■

Therefore, we define the state $\sigma_{ABE}=|\Psi_\sigma\rangle\langle\Psi_\sigma|$, with

$$\begin{aligned} |\Psi_\sigma\rangle = &\frac{1}{\sqrt{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}}(\mathbb{1}_{AE}\otimes\sqrt{Z_\checkmark})(\mathbb{1}_A\otimes U_{BE})|\Psi_\tau\rangle_{AB} \\ &\otimes|0\rangle_E, \end{aligned} \tag{C71}$$

and apply the uncertainty relation on $\sigma_{ABE}$ with the POVMs (C62) and (C63). By computing the states (C59) and (C60) with these choices and by using Eqs. (C64) and (C65), we get

$$\begin{aligned} \sigma_{Z_AE} &= \sum_{j=0}^{d-1}|j\rangle\langle j|_{Z_A}\otimes \mathrm{Tr}_{AB}\left[(M^Z_j\otimes\mathbb{1}_{BE})|\Psi_\sigma\rangle\langle\Psi_\sigma|\right] \\ &= \rho_{Z_AE|1,\Omega_Z}, \end{aligned} \tag{C72}$$

where we used Eq. (C57) and

$$\begin{aligned} \sigma_{X_AB} &= \sum_{k=0}^{d-1}|k\rangle\langle k|_{X_A}\otimes\mathrm{Tr}_{AE}\left[(M^X_k\otimes\mathbb{1}_{BE})|\Psi_\sigma\rangle\langle\Psi_\sigma|\right] \\ &= \frac{1}{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}d}\sum_{k=0}^{d-1}|k\rangle\langle k|_{X_A}\otimes\sqrt{Z_\checkmark}\sigma_k\sqrt{Z_\checkmark}, \end{aligned} \tag{C73}$$

respectively, where we defined $\sigma_k$ as

$$\sigma_k := \mathrm{Tr}_E\left[U_{BE}|1_{X_k}\rangle\langle 1_{X_k}|_B\otimes|0\rangle\langle 0|_E U^\dagger_{BE}\right]. \tag{C74}$$

Note that, because of the assumption (7) and the definition (C51) of yields for rounds with $\Gamma_Z$, we have

$$\begin{aligned} \sum_{k=0}^{d-1}\mathrm{Tr}[Z_\checkmark\sigma_k] &= \sum_{j=0}^{d-1}\Pr(Z_B\neq\emptyset|\Gamma_Z,N_A=1,Z_A=j) \\ &= Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}d, \end{aligned} \tag{C75}$$

which confirms that the state in Eq. (C73) is properly normalized. Thus, the uncertainty relation (C58) yields a lower bound on the entropy of interest:

$$\begin{aligned} H(Z_A|E)_{\rho|1,\Omega_Z} &= H(Z_A|E)_\sigma \\ &\ge \log_2\frac{1}{c} - H(X_A|B)_\sigma, \end{aligned} \tag{C76}$$

where we used Eqs. (C72) and (C66) and where the entropy on the right-hand side is computed on the state (C73). The rest of the proof is devoted to finding an upper bound on $H(X_A|B)_\sigma$ in terms of observed statistics.

Since the entropy $H(X_A|B)_\sigma$ is defined on a classical-quantum state (C73), we can apply a measurement map $\mathcal{E}^X_{B\to\tilde{X}_B}$ on its conditioning system that cannot reduce the entropy [52]:

$$H(X_A|B)_\sigma \le H(X_A|\tilde{X}_B)_{\mathcal{E}^X(\sigma)}, \tag{C77}$$

where $\tilde{X}_B$ is now a classical random variable resulting from a fictitious test measurement. Intuitively, a sensible choice for the fictitious measurement on system $B$ could be Bob's test measurement (C18), defined earlier as the reduced POVM of Bob that focuses on the outcomes of the $X$-basis detector, from which Bob can try to guess the symbol $X_A$ sent by Alice in an $X$-basis round. However, the states of system $B$ in Eq. (C73) undergo a postselection corresponding to a detection in Bob's key generation measurement. This postselection can be described in terms of the first map (C11) composing Bob's key generation measurement map and of the postselection map (C25), such that the state in Eq. (C73) can be recast as

$$\sigma_{X_AB} = \mathrm{Tr}_{\tilde{B}}\circ\mathcal{P}\circ\mathcal{E}^Z_{B\to\tilde{B}B}\left(\frac{1}{d}\sum_{k=0}^{d-1}|k\rangle\langle k|_{X_A}\otimes\sigma_k\right). \tag{C78}$$

Therefore, the application of Bob's test measurement map (C18), $\mathcal{E}^X_{B\to\tilde{B}X_B}$, on the state in Eq. (C78) would *not* return a classical state whose correlations are observed experimentally. In other words, while the state

$$\sigma'_{X_AX_B\tilde{B}} = \mathcal{E}^X_{B\to\tilde{B}X_B}\left(\frac{1}{d}\sum_{k=0}^{d-1}|k\rangle\langle k|_{X_A}\otimes\sigma_k\right) \tag{C79}$$

could be characterized experimentally with traditional QKD techniques such as the decoy-state method, the state

$$\sigma''_{X_A X_B \tilde{B}} = \mathcal{E}^X_{B\to\tilde{B}X_B}\left(\sigma_{X_A B}\right) \tag{C80}$$

cannot, due to the additional maps $\mathrm{Tr}_{\tilde{B}} \circ \mathcal{P} \circ \mathcal{E}^Z_{B\to\tilde{B}B}$ enacting the postselection of a detection in Bob's key generation measurement. According to this observation, the measurement map $\mathcal{E}^X_{B\to\tilde{X}_B}$ to be applied in Eq. (C77) should not be chosen to be Bob's test measurement: $\mathcal{E}^X_{B\to\tilde{X}_B} \neq \mathcal{E}^X_{B\to\tilde{B}X_B}$.

Nevertheless, recall that Bob's test measurement can be decomposed into two CPTP maps (C19), where the first map (C20), $\mathcal{E}^X_{B\to\tilde{B}B}$, is a coarse-grained map that describes only whether there is a detection in the $X$ detector. Let us assume for the moment that the detection probability of Bob's key generation and test measurements coincides for every input state, i.e., the assumption in Eq. (34), which is often implicit in standard QKD security proofs. Under the assumption (34), we observe that the following two maps coincide:

$$\mathrm{Tr}_{\tilde{B}} \circ \mathcal{P} \circ \mathcal{E}^Z_{B\to\tilde{B}B} = \mathrm{Tr}_{\tilde{B}} \circ \mathcal{P} \circ \mathcal{E}^X_{B\to\tilde{B}B}, \tag{C81}$$

i.e., postselection on a detection in the key generation measurement and in the test measurement has the same effect. This fact suggests a better choice for the fictitious measurement ($\mathcal{E}^X_{B\to\tilde{X}_B}$) to be applied on Eq. (C78): the second CPTP map of the decomposition of Bob's test measurement, i.e., the map $\mathcal{E}^X_{\tilde{B}B\to\tilde{B}X_B}$, given in Eq. (C22). More precisely, since the state in Eq. (C78) is already postselected on a detection of the test measurement—provided that the assumption (34) holds—we choose $\mathcal{E}^X_{B\to\tilde{X}_B}$ to be the restriction of $\mathcal{E}^X_{\tilde{B}B\to\tilde{B}X_B}$ to the subspace with $\tilde{B} = 1$:

$$\mathcal{E}^X_{B\to\tilde{X}_B}(\cdot) := \sum_{\tilde{k}=0}^{d-1} \mathrm{Tr}\left[\tilde{X}_{\tilde{k}} \cdot\right] |\tilde{k}\rangle\langle\tilde{k}|_{\tilde{X}_B}, \tag{C82}$$

with $\tilde{X}_{\tilde{k}}$ defined in Eq. (C23). With the above fictitious measurement map and under the assumption (34), the state $\sigma_{X_A B}$ transforms to

$$\begin{aligned}
&\mathcal{E}^X_{B\to\tilde{X}_B}(\sigma_{X_A B}) \\
&= \mathcal{E}^X_{B\to\tilde{X}_B} \circ \mathrm{Tr}_{\tilde{B}} \circ \mathcal{P} \circ \mathcal{E}^Z_{B\to\tilde{B}B}\left(\frac{1}{d}\sum_{k=0}^{d-1} |k\rangle\langle k|_{X_A} \otimes \sigma_k\right) \\
&= \mathcal{E}^X_{B\to\tilde{X}_B} \circ \mathrm{Tr}_{\tilde{B}} \circ \mathcal{P} \circ \mathcal{E}^X_{B\to\tilde{B}B}\left(\frac{1}{d}\sum_{k=0}^{d-1} |k\rangle\langle k|_{X_A} \otimes \sigma_k\right) \\
&= \mathrm{Tr}_{\tilde{B}} \circ \mathcal{P} \circ \mathcal{E}^X_{B\to\tilde{B}X_B}\left(\frac{1}{d}\sum_{k=0}^{d-1} |k\rangle\langle k|_{X_A} \otimes \sigma_k\right) \\
&= \mathrm{Tr}_{\tilde{B}} \circ \mathcal{P}(\sigma'_{X_A X_B \tilde{B}}),
\end{aligned} \tag{C83}$$

which can be characterized experimentally by traditional QKD methods. In our proof, however, we avoid making the assumption in Eq. (34), and hence the classical state arising from $\mathcal{E}^X_{B\to\tilde{X}_B}(\sigma_{X_A B})$, with the fictitious measurement in Eq. (C82), cannot be directly estimated like in most QKD proofs. Nevertheless, we maintain the choice of a fictitious measurement map as given in Eq. (C82), such that our proof can reduce to standard QKD proofs in the special case where the assumption (34) holds.

With our choice of fictitious test measurement, the entropy on the right-hand side of Eq. (C77) is computed on the normalized state:

$$\begin{aligned}
\sigma_{X_A\tilde{X}_B} &= \mathcal{E}^X_{B\to\tilde{X}_B}(\sigma_{X_A B}) \\
&= \sum_{k,\tilde{k}=0}^{d-1} \frac{\mathrm{Tr}\left[\tilde{X}_{\tilde{k}}\sqrt{Z_\checkmark}\sigma_k\sqrt{Z_\checkmark}\right]}{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}d} |k\rangle\langle k|_{X_A} \otimes |\tilde{k}\rangle\langle\tilde{k}|_{\tilde{X}_B},
\end{aligned} \tag{C84}$$

where we used Eq. (C73). Since Eq. (C84) corresponds to a classical-classical state, we can upper-bound its conditional Shannon entropy by using Fano's inequality,

$$H(X_A|\tilde{X}_B)_{\mathcal{E}^X(\sigma)} \leq u(\tilde{e}_{X,1}), \tag{C85}$$

where $u(x)$ is given in Eq. (20) and where we introduced the phase error rate

$$\tilde{e}_{X,1} := \sum_{k=0}^{d-1}\sum_{\tilde{k}\neq k} \frac{\mathrm{Tr}\left[\tilde{X}_{\tilde{k}}\sqrt{Z_\checkmark}\sigma_k\sqrt{Z_\checkmark}\right]}{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}d}. \tag{C86}$$

By combining Eqs. (C76), (C77), and (C85), we obtain the following lower bound on the remaining entropy in Eq. (C56):

$$H(Z_A|E)_{\rho|1,\Omega_Z} \geq \log_2\frac{1}{c} - u(\tilde{e}_{X,1}). \tag{C87}$$

### *c. Reduction of phase error rate*

The derived bound does not yet conclude the proof, since the phase error rate, as defined in Eq. (C86), cannot be directly estimated with the decoy-state method. The reason is that the probability distribution on which the phase error rate is defined is not directly accessible, in general. Indeed, Bob never actually performs the POVM $\{\tilde{X}_{\tilde{k}}\}_{\tilde{k}}$ after postselecting the state on a detection in the key generation measurement. This complication, however, vanishes in the proofs that assume that the detection probability is independent of the measurement basis, as explained in the following remark.

*Remark 2.* Standard QKD security proofs [8,9] assume equality between the detection probabilities of Bob's key

generation measurement (C7) and Bob's test measurement (C15) for any input state. That is, they assume the equality

$$Z_{\checkmark} = X_{\checkmark}, \tag{C88}$$

where $Z_{\checkmark}$ ($X_{\checkmark}$) is the POVM element corresponding to a detection of the key generation (test) measurement. Equipped with the condition in Eq. (C88), one can immediately verify that the phase error rate can be directly estimated from the decoy-state method applied on the statistics of Bob's test measurements, thereby completing the security proof.

To see this, we consider the one-photon bit error rate of Bob's test measurement (C15), which can be defined as

$$\begin{aligned} e_{X,1} &:= \Pr\left(X_A \neq X_B | T = X, N_A = 1, (\eta_\uparrow, \eta_\uparrow), X_B \neq \emptyset\right) \\ &= \sum_{k=0}^{d-1} \sum_{k' \neq k} \Pr(X_A = k, X_B = k' | T = X, \\ &\quad N_A = 1, (\eta_\uparrow, \eta_\uparrow), X_B \neq \emptyset) \\ &= \sum_{k=0}^{d-1} \sum_{k' \neq k} \frac{\mathrm{Tr}[X_{k'} \sigma_k]}{Y^X_{1,(\eta_\uparrow,\eta_\uparrow)} d}, \end{aligned} \tag{C89}$$

where we introduced the one-photon $X$-basis yield:

$$\begin{aligned} &Y^X_{1,(\eta_\uparrow,\eta_\uparrow)} \\ &:= \sum_{k=0}^{d-1} \Pr(X_B \neq \emptyset | T = X, N_A = 1, X_A = k, (\eta_\uparrow, \eta_\uparrow)) \frac{1}{d} \\ &= \sum_{k=0}^{d-1} \frac{1}{d} \mathrm{Tr}\left[(X_{\checkmark} \otimes \mathbb{1}_E) U_{BE} |1_{X_k}\rangle\langle 1_{X_k}|_B \otimes |0\rangle\langle 0|_E U^\dagger_{BE}\right]. \end{aligned} \tag{C90}$$

The one-photon $Z$-basis yield (C51), with Eq. (C39), can be expressed as

$$\begin{aligned} &Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)} \\ &= \sum_{j=0}^{d-1} \frac{1}{d} \mathrm{Tr}\left[(Z_{\checkmark} \otimes \mathbb{1}_E) U_{BE} |1_{Z_j}\rangle\langle 1_{Z_j}|_B \otimes |0\rangle\langle 0|_E U^\dagger_{BE}\right] \\ &= \sum_{k=0}^{d-1} \frac{1}{d} \mathrm{Tr}\left[(X_{\checkmark} \otimes \mathbb{1}_E) U_{BE} |1_{X_k}\rangle\langle 1_{X_k}|_B \otimes |0\rangle\langle 0|_E U^\dagger_{BE}\right] \\ &= Y^X_{1,(\eta_\uparrow,\eta_\uparrow)}, \end{aligned} \tag{C91}$$

where in the second equality we used the assumption in Eq. (C88) together with Eq. (7). At the same time, the assumption in Eq. (C88) allows us to simplify the following expression:

$$\mathrm{Tr}\left[\tilde{X}_{\tilde{k}} \sqrt{Z_{\checkmark}} \sigma_k \sqrt{Z_{\checkmark}}\right] = \mathrm{Tr}[X_{\tilde{k}} \sigma_k], \tag{C92}$$

where we used Eq. (C23). By using Eqs. (C91) and (C92) in the expression for the phase error rate (C86), we obtain

$$\tilde{e}_{X,1} = \sum_{k=0}^{d-1} \sum_{\tilde{k} \neq k} \frac{\mathrm{Tr}[X_{\tilde{k}} \sigma_k]}{Y^X_{1,(\eta_\uparrow,\eta_\uparrow)} d} = e_{X,1}, \tag{C93}$$

i.e., the phase error rate reduces to the bit error rate of Bob's test measurement, which can be estimated with the decoy-state method. This fact would thus conclude the security proof of the protocol, since the phase error rate would be experimentally estimated.

The absence of the assumption (C88) makes the estimation of the phase error rate in Eq. (C86) considerably more challenging in our proof, as it cannot be identified anymore with the bit error rate of Bob's test measurement. In the next subsection we show how we can make use of the full statistics collected in the test rounds to provide an accurate estimation of the phase error rate.

### 4. Phase error rate estimation

In this subsection we develop a method to derive an upper bound on the phase error rate as a function of quantities that can be obtained experimentally with the decoy-state method, without assuming basis-independent detection probabilities, i.e., the assumption in Eq. (C88). For clarity, we report the definition of the phase error rate from Eq. (C86):

$$\tilde{e}_{X,1} = \frac{\sum_{k=0}^{d-1} \sum_{k' \neq k} \mathrm{Tr}\left[\tilde{X}_{k'} \sqrt{Z_{\checkmark}} \sigma_k \sqrt{Z_{\checkmark}}\right]}{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)} d}, \tag{C94}$$

where $Z_{\checkmark}$ is given in Eq. (C12), $\{\sigma_k\}_k$ is given in Eq. (C74), and $\tilde{X}_k$ given in Eq. (C23) and forms a POVM $\{\tilde{X}_k\}_{k=0}^{d-1}$.

We start with a general overview of the argument, after which we detail all the steps of the derivation.

#### *a. Overview of the argument*

Let us consider the subspace with zero photons or one photon localized in $\mathcal{Z}$, which we recall being the set of modes detected by the $Z$-basis detector. For brevity, we name this subspace the "($\leq 1$)-subspace" and label the average state received by Bob, when Alice sends one

photon, as follows:

$$\bar{\sigma} = \sum_{k=0}^{d-1} \frac{\sigma_k}{d} \tag{C95}$$

$$= \sum_{k=0}^{d-1} \mathrm{Tr}_E \left[ U_{BE} \frac{|1_{X_k}\rangle\langle 1_{X_k}|_B}{d} \otimes |0\rangle\langle 0|_E U_{BE}^\dagger \right]$$

$$= \sum_{j=0}^{d-1} \mathrm{Tr}_E \left[ U_{BE} \frac{|1_{Z_j}\rangle\langle 1_{Z_j}|_B}{d} \otimes |0\rangle\langle 0|_E U_{BE}^\dagger \right], \tag{C96}$$

where in the last equality we used Eq. (7).

The first step in estimating the phase error rate consists in reducing the calculation of the phase error rate in Eq. (C86) to the ($\leq 1$)-subspace. The details of this step are provided in Appendixes C 4 b–C 4 e. Indeed, we expect most of the state $\bar{\sigma}$ to lie in the ($\leq 1$)-subspace in an honest implementation of the protocol.

To this aim, we define $\Pi_{\mathcal{Z}}^{\alpha}$ to be the projector of $n = \alpha$ photons in the set $\mathcal{Z}$ and the identity elsewhere, such that the ($\leq 1$)-subspace is the support of $\Pi_{\mathcal{Z}}^{0} + \Pi_{\mathcal{Z}}^{1}$. Then we can express $Z_{\checkmark}$ in terms of $\Pi_{\mathcal{Z}}^{\alpha}$ as follows:

$$Z_{\checkmark} = \sum_{\alpha=0}^{\infty} p_{\checkmark|\alpha} \Pi_{\mathcal{Z}}^{\alpha}, \tag{C97}$$

where $p_{\checkmark|\alpha}$ is the probability that the $Z$-basis detector clicks, given that Bob's input state contains $\alpha$ photons localized in $\mathcal{Z}$. The expression for $p_{\checkmark|\alpha}$ is determined by the dark count probability $p_d^Z$ and the mode-independent detection efficiency $\eta_Z$ of the $Z$-basis detector, as well as the TBS transmittance $\eta_\downarrow$, and is given in Eq. (C181) in Appendix C 4 c (in reality, $p_{\checkmark|\alpha}$ does not depend on $\eta_Z$ since the loss of Bob's $Z$-basis detector is factored out of Bob's apparatus and assigned to the quantum channel; see Appendix C 4 b). By using the expansion (C97) of $Z_{\checkmark}$ in the phase error rate (C86), we can isolate the contribution to the phase error rate given by the fraction of the states $\sigma_k$ existing in the ($\leq 1$)-subspace. We cannot assume that the states $\sigma_k$ are completely confined to that subspace due to potential attacks by Eve, which may, for example, add photons to Alice's pulses. Therefore, in Appendix C 4 d we show how to use the detection statistics of the $Z$-basis detector, with the TBS settings $(\eta_\downarrow, \eta_\downarrow)$, $(\eta_\uparrow, \eta_\uparrow)$, and $(\eta_2, \eta_2)$, to derive an upper bound on the weight of $\bar{\sigma}$ outside the ($\leq 1$)-subspace. Our method draws inspiration from the detector decoy technique [28] and leads to the following bound [see Eq. (C217) in Appendix C 4 d]:

$$\sum_{\alpha=2}^{\infty} \mathrm{Tr}[\bar{\sigma}\, \Pi_{\mathcal{Z}}^{\alpha}] \leq \overline{w}_{\mathcal{Z}}^{>1}, \tag{C98}$$

where $\overline{w}_{\mathcal{Z}}^{>1}$ is reported in Eq. (C218) in terms of quantities that can be directly estimated with the decoy-state method (the $Z$-basis yields). In Appendix C 4 e we obtain the following upper bound on the phase error rate (C86), which uses Eqs. (C97) and (C98) to reduce the evaluation of the error rate to the ($\leq 1$)-subspace [see Eq. (C247) in Appendix C 4 e]:

$$\tilde{e}_{X,1} Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)} \leq \frac{1}{d} \sum_{k=0}^{d-1} \mathrm{Tr}\left[ \sigma_k M_{\mathcal{Z}}^{\leq 1} \sum_{k' \neq k} \tilde{X}_{k'} M_{\mathcal{Z}}^{\leq 1} \right] + \overline{\Delta_2} + \overline{w}_{\mathcal{Z}}^{>1}, \tag{C99}$$

where $\overline{\Delta_2}$ is a function of $\overline{w}_{\mathcal{Z}}^{>1}$ and $Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}$ given in Eq. (C248), and where the support of the operator

$$M_{\mathcal{Z}}^{\leq 1} = \sqrt{p_{\checkmark|0}}\, \Pi_{\mathcal{Z}}^{0} + \sqrt{p_{\checkmark|1}}\, \Pi_{\mathcal{Z}}^{1} \tag{C100}$$

is the ($\leq 1$)-subspace.

In Appendix C 4 j, we simplify the expression in Eq. (C99) by computing explicitly the POVM element $\tilde{X}_k$ given in Eq. (30). To this aim, similarly to the introduction of $\Pi_{\mathcal{Z}}^{\alpha}$ for the $Z$-basis detector, we introduce the projector $\Pi_{\mathcal{X}}^{\beta}$, which projects on the subspace with $\beta$ photons in the set of modes $\mathcal{X}$ and acts as the identity elsewhere. Then the POVM element $X_k$ of Bob's test measurement can be written in terms of (1) projectors similar to $\Pi_{\mathcal{X}}^{\beta}$, (2) the total dark count probability ($p_d^{\mathcal{X}}$) of the $X$-basis detector, (3) the TBS transmittance $\eta_\uparrow$, and (4) the ratio between the mode-independent detection efficiency of the $X$-basis detector and the mode-independent detection efficiency of the $Z$-basis detector (since we factored out the efficiency of the $Z$-basis detector):

$$\eta_r = \frac{\eta_X}{\eta_Z}. \tag{C101}$$

Note that, by assumption, $\eta_r \leq 1$. The calculation of $\tilde{X}_k$ in Appendix C 4 j leads to the following operator upper bound [see Eq. (C386)]:

$$\sum_{k' \neq k} \tilde{X}_{k'} \leq \frac{\sum_{k' \neq k} X_{k'}}{p_d^{\mathcal{X}} + \eta_r \eta_\uparrow (1 - p_d^{\mathcal{X}})} + \frac{\eta_r \eta_\uparrow (1 - p_d^{\mathcal{X}})}{p_d^{\mathcal{X}} + \eta_r \eta_\uparrow (1 - p_d^{\mathcal{X}})} \Pi_{\mathcal{X}}^{0}. \tag{C102}$$

When this is used in Eq. (C99), it yields the following upper bound on the phase error rate:

$$\tilde{e}_{X,1} Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)} \leq \frac{\sum_{k=0}^{d-1} \mathrm{Tr}\left[ \frac{\sigma_k}{d} M_{\mathcal{Z}}^{\leq 1} \sum_{k' \neq k} X_{k'} M_{\mathcal{Z}}^{\leq 1} \right]}{p_d^{\mathcal{X}} + \eta_r \eta_\uparrow (1 - p_d^{\mathcal{X}})} + \frac{\eta_r \eta_\uparrow (1 - p_d^{\mathcal{X}})}{p_d^{\mathcal{X}} + \eta_r \eta_\uparrow (1 - p_d^{\mathcal{X}})} \mathrm{Tr}\left[ \bar{\sigma} M_{\mathcal{Z}}^{\leq 1} \Pi_{\mathcal{X}}^{0} M_{\mathcal{Z}}^{\leq 1} \right] + \overline{\Delta_2} + \overline{w}_{\mathcal{Z}}^{>1}. \tag{C103}$$

We now focus on estimating the first term on the right-hand side of Eq. (C103). This term is clearly linked to the one-photon bit error rate of Bob's test measurement, Eq. (35). However, note that we must estimate such an error rate when restricting the input state to the $(\leq 1)$-subspace, due to the presence of the operator $M_{\mathcal{Z}}^{\leq 1}$. To this aim, we introduce the one-photon $X$-basis bit error rates $e_{X,1,(\eta_i,\eta_l),\checkmark}$ and $e_{X,1,(\eta_i,\eta_l),\emptyset}$, which we simply refer to as the "test-round bit error rates" and that correspond to the bit error rate in the $X$ basis when the $Z$-basis detector has a detection or no detection, respectively. They can be expressed as follows [see Eqs. (C274) and (C275) in Appendix C 4 f]:

$$e_{X,1,(\eta_i,\eta_l),\checkmark} = \frac{\sum_{k=0}^{d-1} \mathrm{Tr}\left[\frac{\sigma_k}{d}\sum_{k'\neq k} X_{k',\checkmark}^{(\eta_i,\eta_l)}\right]}{Y_{1,(\eta_i,\eta_l)}^{X,\checkmark}}, \tag{C104}$$

$$e_{X,1,(\eta_i,\eta_l),\emptyset} = \frac{\sum_{k=0}^{d-1} \mathrm{Tr}\left[\frac{\sigma_k}{d}\sum_{k'\neq k} X_{k',\emptyset}^{(\eta_i,\eta_l)}\right]}{Y_{1,(\eta_i,\eta_l)}^{X,\emptyset}}, \tag{C105}$$

where we call $Y_{1,(\eta_i,\eta_l)}^{X,\checkmark}$ and $Y_{1,(\eta_i,\eta_l)}^{X,\emptyset}$ the "test-round yields" and where $X_{k',\checkmark}^{(\eta_i,\eta_l)}$ ($X_{k',\emptyset}^{(\eta_i,\eta_l)}$) is Bob's POVM element describing a detection of outcome $k'$ in the $X$-basis detector and a detection (no detection) in the $Z$-basis detector, given that the TBS is set to $(\eta_i,\eta_l)$. See Appendix A for a precise definition of the test-round yields and bit error rates. Note that, with this formalism, by definition it holds that

$$X_{k'} = X_{k',\checkmark}^{(\eta_\uparrow,\eta_\uparrow)} + X_{k',\emptyset}^{(\eta_\uparrow,\eta_\uparrow)}. \tag{C106}$$

The two test-round bit error rates contain more information about the protocol's statistics than the bit error rate of Bob's test measurement alone, Eq. (C93), and this will be crucial to accurately estimate the phase error rate.

Similarly to the bound on the phase error rate in Eq. (C99) through the expansion (C97), we can use the relation: $\mathbb{1} = \Pi_{\mathcal{Z}}^{\leq 1} + \Pi_{\mathcal{Z}}^{>1}$, with $\Pi_{\mathcal{Z}}^{\leq 1} = \Pi_{\mathcal{Z}}^{0} + \Pi_{\mathcal{Z}}^{1}$, to isolate the contribution of the $(\leq 1)$-subspace to the test-round bit error rates (C104) and (C105). We do so in Appendix C 4 g, where we obtain in Eqs. (C286) and (C290) tight upper and lower bounds on the following quantities:

$$\left[Y_{1,(\eta_i,\eta_l)}^{X,\checkmark} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]_{\mathcal{Z}}^{\leq 1} = \sum_{k=0}^{d-1} \mathrm{Tr}\left[\frac{\sigma_k}{d}\Pi_{\mathcal{Z}}^{\leq 1}\sum_{k'\neq k} X_{k',\checkmark}^{(\eta_i,\eta_l)}\Pi_{\mathcal{Z}}^{\leq 1}\right], \tag{C107}$$

$$\left[Y_{1,(\eta_i,\eta_l)}^{X,\emptyset} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]_{\mathcal{Z}}^{\leq 1} = \sum_{k=0}^{d-1} \mathrm{Tr}\left[\frac{\sigma_k}{d}\Pi_{\mathcal{Z}}^{\leq 1}\sum_{k'\neq k} X_{k',\emptyset}^{(\eta_i,\eta_l)}\Pi_{\mathcal{Z}}^{\leq 1}\right], \tag{C108}$$

where the notation $[\cdot]_{\mathcal{Z}}^{\leq 1}$ indicates that the enclosed quantity is calculated only in the $(\leq 1)$-subspace. The bounds on the above quantities are reported in Eqs. (B26)–(B29). Importantly, they can be directly estimated from the protocol's statistics, as they are given in terms of the test-round yields and bit error rates as well as of $\overline{w}_{\mathcal{Z}}^{>1}$.

Unfortunately, the restricted test-round bit error rates in Eqs. (C107) and (C108) cannot be directly used to quantify the first term on the right-hand side of Eq. (C103). This is because the latter is restricted to the $(\leq 1)$-subspace by the operator in Eq. (C100), while the error rates in Eqs. (C107) and (C108) are restricted to the same subspace via the projector $\Pi_{\mathcal{Z}}^{\leq 1}$.

This prompts us to expand both the term in Eq. (C103) and the restricted test-round bit error rates with Eq. (C100) and $\Pi_{\mathcal{Z}}^{\leq 1} = \Pi_{\mathcal{Z}}^{0} + \Pi_{\mathcal{Z}}^{1}$, respectively, such that each term in the expansion contains either a projection on $\Pi_{\mathcal{Z}}^{0}$, or a projection on $\Pi_{\mathcal{Z}}^{1}$, or the off-diagonal blocks. For the restricted test-round bit error rates, we obtain

$$\left[Y_{1,(\eta_i,\eta_l)}^{X,\checkmark} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]_{\mathcal{Z}}^{\leq 1} = \left[Y_{1,(\eta_i,\eta_l)}^{X,\checkmark} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]_{\mathcal{Z}}^{0} + \left[Y_{1,(\eta_i,\eta_l)}^{X,\checkmark} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]_{\mathcal{Z}}^{0,1} + \left[Y_{1,(\eta_i,\eta_l)}^{X,\checkmark} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]_{\mathcal{Z}}^{1}, \tag{C109}$$

$$\left[Y_{1,(\eta_i,\eta_l)}^{X,\emptyset} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]_{\mathcal{Z}}^{\leq 1} = \left[Y_{1,(\eta_i,\eta_l)}^{X,\emptyset} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]_{\mathcal{Z}}^{0} + \left[Y_{1,(\eta_i,\eta_l)}^{X,\emptyset} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]_{\mathcal{Z}}^{0,1} + \left[Y_{1,(\eta_i,\eta_l)}^{X,\emptyset} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]_{\mathcal{Z}}^{1}, \tag{C110}$$

where we defined

$$\left[Y_{1,(\eta_i,\eta_l)}^{X,\checkmark} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]_{\mathcal{Z}}^{\alpha} = \sum_{k=0}^{d-1} \mathrm{Tr}\left[\frac{\sigma_k}{d}\Pi_{\mathcal{Z}}^{\alpha}\sum_{k'\neq k} X_{k',\checkmark}^{(\eta_i,\eta_l)}\Pi_{\mathcal{Z}}^{\alpha}\right], \tag{C111}$$

$$\left[Y_{1,(\eta_i,\eta_l)}^{X,\checkmark} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]_{\mathcal{Z}}^{0,1} = \sum_{k=0}^{d-1} \mathrm{Tr}\left[\frac{\sigma_k}{d}\left(\Pi_{\mathcal{Z}}^{0}\sum_{k'\neq k} X_{k',\checkmark}^{(\eta_i,\eta_l)}\Pi_{\mathcal{Z}}^{1} + \mathrm{H.c.}\right)\right] \tag{C112}$$

for $\alpha = 0, 1$, and similarly for the terms relative to no click in the $Z$-basis detector. We note that Eq. (C112) is not null, in general, since the POVM elements $X_{k',\checkmark}^{(\eta_i,\eta_l)}$ are not necessarily block diagonal in the subspaces defined by $\Pi_{\mathcal{Z}}^{\alpha}$.

For the first term on the right-hand side of Eq. (C103), the expansion through Eq. (C100) produces the following expression:

$$\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}M_{\mathcal{Z}}^{\leq 1}\sum_{k'\neq k}X_{k'}M_{\mathcal{Z}}^{\leq 1}\right]=\sum_{\alpha=0}^{1}p_{\checkmark|\alpha}\left(\left[Y^{X,\checkmark}_{1,(\eta_\uparrow,\eta_\uparrow)}e_{X,1,(\eta_\uparrow,\eta_\uparrow),\checkmark}\right]^{\alpha}_{\mathcal{Z}}+\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_\uparrow)}e_{X,1,(\eta_\uparrow,\eta_\uparrow),\emptyset}\right]^{\alpha}_{\mathcal{Z}}\right)$$
$$+\sqrt{p_{\checkmark|0}p_{\checkmark|1}}\left(\left[Y^{X,\checkmark}_{1,(\eta_\uparrow,\eta_\uparrow)}e_{X,1,(\eta_\uparrow,\eta_\uparrow),\checkmark}\right]^{0,1}_{\mathcal{Z}}+\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_\uparrow)}e_{X,1,(\eta_\uparrow,\eta_\uparrow),\emptyset}\right]^{0,1}_{\mathcal{Z}}\right),\tag{C113}$$

where we used the definitions (C111) and (C112) and the equality (C106).

By comparing the expansions of the restricted test-round bit error rates (C109) and (C110) with the expansion (C113) of the term coming from the right-hand side of Eq. (C103), we conclude that an accurate estimation of the latter requires individually estimating each of the three terms in the expansions (C109) and (C110) of the restricted test-round bit error rates.

The method that we use to estimate each of the three terms on the right-hand side of Eqs. (C109) and (C110) represents one of the novelties of our security proof. The method is based on the observation that when the state (on which the three terms are computed) is projected on the subspaces with zero photons or one photon in $\mathcal{Z}$, then the unitary action of the TBS on the photons localized in $\mathcal{Z}$ can be factored out and reduces to a simple prefactor.

More specifically, recall that the TBS setting $(\eta_i,\eta_l)$ means that the TBS acts as a beam splitter with transmittance $\eta_i$ ($\eta_l$) for photons localized in (outside) $\mathcal{Z}$. For illustrative purposes, let us consider the term $\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{1}_{\mathcal{Z}}$, which can be interpreted as the probability of the following intersection of events [averaged over Alice's random selection of the symbol $X_A=k$): the input state $\sigma_k$ of Bob contains one photon localized in $\mathcal{Z}$, the $Z$-basis detector clicks, and the $X$-basis detector clicks with an erroneous outcome $k'\neq k$ (all with the TBS setting $(\eta_i,\eta_l)$]. By following Fig. 1, we see that either the single photon localized in $\mathcal{Z}$ is transmitted by the TBS with probability $\eta_i$, in which case the $Z$-basis detector click is caused by a dark count, or the photon is reflected by the TBS with probability $1-\eta_i$, causing a click in the $Z$-basis detector (recall that the efficiency $\eta_Z$ of the $Z$-basis detector is factored out in the quantum channel). Besides, the erroneous outcome in the $X$-basis detector could be caused by the transmitted photon localized in $\mathcal{Z}$, but also by a dark count or by any number of photons not localized in $\mathcal{Z}$. Then, the probability term that we considered can be expressed as a sum of two terms corresponding to the scenarios with the transmitted or reflected photon:

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{1}_{\mathcal{Z}}=p_d^{\mathcal{Z}}\eta_i\,\mathbb{E}^{1t}_{\eta_l}+(1-\eta_i)\,\mathbb{E}^{1r}_{\eta_l},\tag{C114}$$

where the action of the TBS on the single photon in $\mathcal{Z}$ is made explicit by the prefactors $\eta_i$ and $1-\eta_i$. In Eq. (C114), the quantities $\mathbb{E}^{1t}_{\eta_l}$ and $\mathbb{E}^{1r}_{\eta_l}$ depend on the input states $\sigma_k$ and their interaction with the $X$-basis detector, but also nontrivially depend on the TBS transmittance $\eta_l$—indeed, $\sigma_k$ can contain an arbitrary number of photons outside $\mathcal{Z}$. In Appendix C 4 h we provide a rigorous proof of the result in Eq. (C114) and derive similar decompositions for the other terms in Eqs. (C109) and (C110) [see Eqs. (C350)–(C355)]:

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{0}_{\mathcal{Z}}=p_d^{\mathcal{Z}}\,\mathbb{E}^{0}_{\eta_l},\tag{C115}$$

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{0}_{\mathcal{Z}}=(1-p_d^{\mathcal{Z}})\,\mathbb{E}^{0}_{\eta_l},\tag{C116}$$

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{0,1}_{\mathcal{Z}}=p_d^{\mathcal{Z}}\sqrt{\eta_i}\,\mathbb{E}^{0,1}_{\eta_l},\tag{C117}$$

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{0,1}_{\mathcal{Z}}=(1-p_d^{\mathcal{Z}})\sqrt{\eta_i}\,\mathbb{E}^{0,1}_{\eta_l},\tag{C118}$$

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{1}_{\mathcal{Z}}=(1-p_d^{\mathcal{Z}})\eta_i\,\mathbb{E}^{1t}_{\eta_l},\tag{C119}$$

where again the action of the TBS on the photon localized in $\mathcal{Z}$ is singled out by the factors containing $\eta_i$.

The notable fact from Eqs. (C114)–(C119) is that $\eta_i$ is factored out of the variables $\mathbb{E}^{0}_{\eta_l}$, $\mathbb{E}^{0,1}_{\eta_l}$, $\mathbb{E}^{1r}_{\eta_l}$, and $\mathbb{E}^{1t}_{\eta_l}$. Therefore, any choice of $\eta_i$ affects the test-round bit error rates only through the coefficients with which the variables $\mathbb{E}^{0}_{\eta_l}$, $\mathbb{E}^{0,1}_{\eta_l}$, $\mathbb{E}^{1r}_{\eta_l}$, and $\mathbb{E}^{1t}_{\eta_l}$ appear in Eqs. (C114)–(C119). Thus, by using Eqs. (C114)–(C119) in the expansions (C109) and (C110), we can derive a linear system of equations [see Eq. (C356)]

$$\begin{cases}\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{\leq 1}_{\mathcal{Z}} &= p_d^{\mathcal{Z}}\left(\mathbb{E}^{0}_{\eta_l}+\sqrt{\eta_i}\,\mathbb{E}^{0,1}_{\eta_l}+\eta_i\,\mathbb{E}^{1t}_{\eta_l}\right)+(1-\eta_i)\,\mathbb{E}^{1r}_{\eta_l},\\ \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}} &= (1-p_d^{\mathcal{Z}})\left(\mathbb{E}^{0}_{\eta_l}+\sqrt{\eta_i}\,\mathbb{E}^{0,1}_{\eta_l}+\eta_i\,\mathbb{E}^{1t}_{\eta_l}\right)\end{cases}\tag{C120}$$

in the variables $\mathbb{E}^0_{\eta_l}$, $\mathbb{E}^{0,1}_{\eta_l}$, $\mathbb{E}^{1r}_{\eta_l}$, and $\mathbb{E}^{1t}_{\eta_l}$ by simply choosing different values of $\eta_i$. In particular, each equation in the above system corresponds to three different equations depending on the setting $\eta_i \in \{\eta_\uparrow, \eta_\downarrow, \eta_2\}$. Note that the left-hand sides, i.e., the test-round bit error rates restricted to the $(\leq 1)$-subspace (C107) and (C108), can be considered as known quantities since they have been tightly bounded with upper and lower bounds that are given in terms of observed statistics.

In Appendix C 4 i, we solve the linear system in Eq. (C120) and provide the solution for $\mathbb{E}^0_{\eta_l}$, $\mathbb{E}^{0,1}_{\eta_l}$, $\mathbb{E}^{1r}_{\eta_l}$, and $\mathbb{E}^{1t}_{\eta_l}$ in terms of the test-round bit error rates restricted to the $(\leq 1)$-subspace. Subsequently, we replace the latter with their respective upper or lower bound in such a way that the resulting expressions are upper bounds on the quantities $\mathbb{E}^0_{\eta_l}$, $\mathbb{E}^{0,1}_{\eta_l}$, $\mathbb{E}^{1r}_{\eta_l}$, and $\mathbb{E}^{1t}_{\eta_l}$. We indicate such bounds with $\overline{\mathbb{E}}^0_{\eta_l}$, $\overline{\mathbb{E}}^{0,1}_{\eta_l}$, $\overline{\mathbb{E}}^{1r}_{\eta_l}$, and $\overline{\mathbb{E}}^{1t}_{\eta_l}$ and report them in Eqs. (B22)–(B25). The variables $\mathbb{E}^0_{\eta_l}$, $\mathbb{E}^{0,1}_{\eta_l}$, $\mathbb{E}^{1r}_{\eta_l}$, and $\mathbb{E}^{1t}_{\eta_l}$ appear with positive signs in the phase error rate and thus should be replaced by their upper bounds if they cannot be computed explicitly.

We can now use the bounds $\overline{\mathbb{E}}^0_{\eta_l}$, $\overline{\mathbb{E}}^{0,1}_{\eta_l}$, $\overline{\mathbb{E}}^{1r}_{\eta_l}$, and $\overline{\mathbb{E}}^{1t}_{\eta_l}$ to obtain an upper bound on the first term of the phase error rate bound in Eq. (C103). Indeed, by combining Eqs. (C114)–(C119) with Eq. (C113), we obtain the upper bound:

$$\begin{aligned}&\textstyle\sum_{k=0}^{d-1} \mathrm{Tr}\left[\frac{\sigma_k}{d} M_{\mathcal{Z}}^{\leq 1} \sum_{k'\neq k} X_{k'} M_{\mathcal{Z}}^{\leq 1}\right] \\ &\quad \leq p_{\checkmark|0}\overline{\mathbb{E}}^0_{\eta_\uparrow} + \sqrt{p_{\checkmark|0}p_{\checkmark|1}}\sqrt{\eta_\uparrow}\overline{\mathbb{E}}^{0,1}_{\eta_\uparrow} \\ &\qquad + p_{\checkmark|1}\left(\eta_\uparrow \overline{\mathbb{E}}^{1t}_{\eta_\uparrow} + (1-\eta_\uparrow)\overline{\mathbb{E}}^{1r}_{\eta_\uparrow}\right), \end{aligned} \tag{C121}$$

where each quantity on the right-hand side is either known or directly expressed in terms of observed statistics. Recall that $p_{\checkmark|\alpha}$ was introduced after Eq. (C97).

The remaining term to be estimated, in order to complete the estimation of the phase error rate, is the second term in the phase error rate bound (C103), which can be interpreted as the weight of the average state received by Bob in the subspace with zero photons in the modes $\mathcal{X}$, restricted to the $(\leq 1)$-subspace. By expanding it through Eq. (C100), we obtain three terms

$$\begin{aligned}\mathrm{Tr}\left[\bar{\sigma} M_{\mathcal{Z}}^{\leq 1} \Pi^0_{\mathcal{X}} M_{\mathcal{Z}}^{\leq 1}\right] &= p_{\checkmark|0}\,\mathrm{Tr}\left[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^0_{\mathcal{Z}}\right] \\ &+ \sqrt{p_{\checkmark|0}p_{\checkmark|1}}\,\mathrm{Tr}\left[\bar{\sigma}\left(\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}} + \mathrm{H.c.}\right)\right] \\ &+ p_{\checkmark|1}\,\mathrm{Tr}\left[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right], \end{aligned} \tag{C122}$$

corresponding to the projections in the subspaces of $\Pi^0_{\mathcal{Z}}$, and $\Pi^1_{\mathcal{Z}}$, or the off-diagonal term. We deduce that a correct estimation of the term of interest requires estimating individually the three terms on the right-hand side of Eq. (C122). To this aim, we need to combine two methods that have already been used in the proof, namely, the detector decoy technique [used to extract the weight of $\bar{\sigma}$ outside the $(\leq 1)$-subspace with Eq. (C98)] and the method based on linear equations [used to estimate the single terms in the expansion (C113)]. For this reason, the accurate estimation of the three terms in Eq. (C122) can be seen as the more sophisticated procedure of the whole proof.

The first step considers the test-round yields $Y^{X,\checkmark}_{1,(\eta_l,\eta_l)}$ and $Y^{X,\emptyset}_{1,(\eta_l,\eta_l)}$, i.e., the probability that the $X$-basis detector clicks and the $Z$-basis detector clicks or does not click, respectively (see Appendix A). Their sum can be expressed in terms of Bob's POVM elements:

$$Y^{X,\checkmark}_{1,(\eta_l,\eta_l)} + Y^{X,\emptyset}_{1,(\eta_l,\eta_l)} = \mathrm{Tr}\left[\bar{\sigma}\sum_{k=0}^{d-1}\left(X^{(\eta_l,\eta_l)}_{k,\checkmark} + X^{(\eta_l,\eta_l)}_{k,\emptyset}\right)\right]. \tag{C123}$$

In Appendix C 4 f we show that the following equality holds:

$$\begin{aligned}&\textstyle\sum_{k=0}^{d-1} X^{(\eta_l,\eta_l)}_{k,\checkmark} + X^{(\eta_l,\eta_l)}_{k,\emptyset} \\ &\quad = \textstyle\sum_{\beta=0}^{\infty}\left[1-(1-p_d^{\mathcal{X}})(1-\eta_r\eta_l)^\beta\right]\Pi^\beta_{\mathcal{X}}, \end{aligned} \tag{C124}$$

which can be seen as the POVM element corresponding to a detection in the $X$-basis detector when the TBS setting is $(\eta_l, \eta_l)$. From the last expression, we can immediately obtain the POVM element describing no detection in the $X$-basis detector:

$$\begin{aligned}&\mathbb{1} - \textstyle\sum_{k=0}^{d-1}\left(X^{(\eta_l,\eta_l)}_{k,\checkmark} + X^{(\eta_l,\eta_l)}_{k,\emptyset}\right) \\ &\quad = (1-p_d^{\mathcal{X}})\textstyle\sum_{\beta=0}^{\infty}(1-\eta_r\eta_l)^\beta\Pi^\beta_{\mathcal{X}}, \end{aligned} \tag{C125}$$

where we used the fact that $\sum_{\beta=0}^{\infty}\Pi^\beta_{\mathcal{X}} = \mathbb{1}$. Now, we realize that the three terms in Eq. (C122) can be recovered from the right-hand side of Eq. (C125) if we project the operator on the subspaces of $\Pi^0_{\mathcal{Z}}$ or $\Pi^1_{\mathcal{Z}}$. By doing so on both sides of the operator equation in Eq. (C125), we obtain

$$\begin{aligned}&\Pi^\alpha_{\mathcal{Z}} - \Pi^\alpha_{\mathcal{Z}}\left(\textstyle\sum_{k=0}^{d-1} X^{(\eta_l,\eta_l)}_{k,\checkmark} + X^{(\eta_l,\eta_l)}_{k,\emptyset}\right)\Pi^\alpha_{\mathcal{Z}} \\ &\quad = (1-p_d^{\mathcal{X}})\textstyle\sum_{\beta=0}^{\infty}(1-\eta_r\eta_l)^\beta\Pi^\alpha_{\mathcal{Z}}\Pi^\beta_{\mathcal{X}}\Pi^\alpha_{\mathcal{Z}} \end{aligned} \tag{C126}$$

for $\alpha = 0, 1$. We can now take the expectation value of the operator in Eq. (C126) on the state $\bar{\sigma}$ and obtain the following equation, which contains two of the three terms in Eq. (C122):

$$\mathrm{Tr}[\bar{\sigma}\,\Pi^{\alpha}_{\mathcal{Z}}] - \left(\left[Y^{X,\checkmark}_{1,(\eta_l,\eta_l)}\right]^{\alpha}_{\mathcal{Z}} + \left[Y^{X,\emptyset}_{1,(\eta_l,\eta_l)}\right]^{\alpha}_{\mathcal{Z}}\right) = (1-p_d^{\mathcal{X}})\sum_{\beta=0}^{\infty}(1-\eta_r\eta_l)^{\beta}\,\mathrm{Tr}\left[\bar{\sigma}\,\Pi^{\alpha}_{\mathcal{Z}}\Pi^{\beta}_{\mathcal{X}}\Pi^{\alpha}_{\mathcal{Z}}\right], \tag{C127}$$

where we introduced, similarly to Eq. (C111), the test-round yields of the states projected on the subspaces of $\Pi^0_{\mathcal{Z}}$ and $\Pi^1_{\mathcal{Z}}$ (for $\alpha = 0, 1$),

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{\alpha}_{\mathcal{Z}} = \mathrm{Tr}\left[\bar{\sigma}\,\Pi^{\alpha}_{\mathcal{Z}}\textstyle\sum_{k=0}^{d-1}X^{(\eta_i,\eta_l)}_{k,\checkmark}\,\Pi^{\alpha}_{\mathcal{Z}}\right], \tag{C128}$$

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\alpha}_{\mathcal{Z}} = \mathrm{Tr}\left[\bar{\sigma}\,\Pi^{\alpha}_{\mathcal{Z}}\textstyle\sum_{k=0}^{d-1}X^{(\eta_i,\eta_l)}_{k,\emptyset}\,\Pi^{\alpha}_{\mathcal{Z}}\right]. \tag{C129}$$

We now show that the left-hand side of Eq. (C127) is known by linking it to observed quantities. In particular, the quantity $\mathrm{Tr}[\bar{\sigma}\,\Pi^{\alpha}_{\mathcal{Z}}]$ is nothing more than the weight of the average state received by Bob in the subspace with $\alpha$ photons in $\mathcal{Z}$. In Appendix C 4 d, in a manner similar to the derivation of the bound in Eq. (C98), we use the detector decoy technique [28] to obtain tight upper ($\overline{w}^{\alpha}_{\mathcal{Z}}$) and lower ($\underline{w}^{\alpha}_{\mathcal{Z}}$) bounds on $\mathrm{Tr}[\bar{\sigma}\,\Pi^{\alpha}_{\mathcal{Z}}]$ in terms of quantities estimated with the decoy-state method—the $Z$-basis yields. The bounds are reported in Eqs. (B6)–(B9).

In parallel, we can again use the relation $\mathbb{1} = \Pi^{\leq 1}_{\mathcal{Z}} + \Pi^{>1}_{\mathcal{Z}}$, with $\Pi^{\leq 1}_{\mathcal{Z}} = \Pi^{0}_{\mathcal{Z}} + \Pi^{1}_{\mathcal{Z}}$, to isolate the contribution of the ($\leq 1$)-subspace to the test-round yields in Eq. (C123). In particular, in Appendix C 4 g we derive tight upper and lower bounds [summarized in Eqs. (B18)–(B21)] on the left-hand sides of the equalities

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} = \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0}_{\mathcal{Z}} + \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}} + \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{1}_{\mathcal{Z}}, \tag{C130}$$

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} = \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{0}_{\mathcal{Z}} + \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}} + \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{1}_{\mathcal{Z}} \tag{C131}$$

in terms of observed statistics and of $\overline{w}^{>1}_{\mathcal{Z}}$, where we defined

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}} = \mathrm{Tr}\left[\bar{\sigma}\left(\Pi^{0}_{\mathcal{Z}}\textstyle\sum_{k=0}^{d-1}X^{(\eta_i,\eta_l)}_{k,\checkmark}\,\Pi^{1}_{\mathcal{Z}} + \mathrm{H.c.}\right)\right], \tag{C132}$$

and similarly for the case with no $Z$-basis detection.

With the same argument as used in Eqs. (C114) to single out the effect of the TBS on the single photon localized in $\mathcal{Z}$, we can express the test-round yields projected by $\Pi^{\alpha}_{\mathcal{Z}}$ in terms of some variables $\mathbb{Y}^0_{\eta_l}$, $\mathbb{Y}^{0,1}_{\eta_l}$, $\mathbb{Y}^{1t}_{\eta_l}$, and $\mathbb{Y}^{1r}_{\eta_l}$ as [see Eq. (C327) and thereafter in Appendix C 4 h]

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0}_{\mathcal{Z}} = p_d^{\mathcal{Z}}\,\mathbb{Y}^0_{\eta_l}, \tag{C133}$$

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{0}_{\mathcal{Z}} = (1-p_d^{\mathcal{Z}})\,\mathbb{Y}^0_{\eta_l}, \tag{C134}$$

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}} = p_d^{\mathcal{Z}}\sqrt{\eta_i}\,\mathbb{Y}^{0,1}_{\eta_l}, \tag{C135}$$

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}} = (1-p_d^{\mathcal{Z}})\sqrt{\eta_i}\,\mathbb{Y}^{0,1}_{\eta_l}, \tag{C136}$$

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{1}_{\mathcal{Z}} = p_d^{\mathcal{Z}}\,\eta_i\,\mathbb{Y}^{1t}_{\eta_l} + (1-\eta_i)\,\mathbb{Y}^{1r}_{\eta_l}, \tag{C137}$$

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{1}_{\mathcal{Z}} = (1-p_d^{\mathcal{Z}})\eta_i\,\mathbb{Y}^{1t}_{\eta_l} \tag{C138}$$

such that Eqs. (C130) and (C131) can be interpreted as a linear system in the variables $\mathbb{Y}^0_{\eta_l}$, $\mathbb{Y}^{0,1}_{\eta_l}$, $\mathbb{Y}^{1t}_{\eta_l}$, and $\mathbb{Y}^{1r}_{\eta_l}$ [see Eq. (C337)]:

$$\begin{cases} \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} &= p_d^{\mathcal{Z}}\left(\mathbb{Y}^0_{\eta_l} + \sqrt{\eta_i}\,\mathbb{Y}^{0,1}_{\eta_l} + \eta_i\,\mathbb{Y}^{1t}_{\eta_l}\right) + (1-\eta_i)\,\mathbb{Y}^{1r}_{\eta_l}, \\ \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} &= (1-p_d^{\mathcal{Z}})\left(\mathbb{Y}^0_{\eta_l} + \sqrt{\eta_i}\,\mathbb{Y}^{0,1}_{\eta_l} + \eta_i\,\mathbb{Y}^{1t}_{\eta_l}\right), \end{cases} \tag{C139}$$

where each of the equations actually corresponds to three equations depending on the choice of $\eta_i \in \{\eta_\uparrow, \eta_\downarrow, \eta_2\}$. In Appendix C 4 i we solve the system in Eq. (C139) for the variables $\mathbb{Y}^0_{\eta_l}$, $\mathbb{Y}^{0,1}_{\eta_l}$, $\mathbb{Y}^{1t}_{\eta_l}$, and $\mathbb{Y}^{1r}_{\eta_l}$. Given that we previously obtained tight upper and lower bounds on the left-hand sides of the system, this translates to accurate upper and lower bounds on the variables $\mathbb{Y}^0_{\eta_l}$, $\mathbb{Y}^{0,1}_{\eta_l}$, $\mathbb{Y}^{1t}_{\eta_l}$, and $\mathbb{Y}^{1r}_{\eta_l}$, reported in Eqs. (B12)–(B17).

We have thus argued how to obtain good bounds on the terms on the left-hand side of Eq. (C127). By using Eqs. (C133)–(C138) in Eq. (C127), we can express the equation for the case $\alpha = 0$ as

$$\mathrm{Tr}[\bar{\sigma}\,\Pi^{0}_{\mathcal{Z}}] - \mathbb{Y}^0_{\eta_l} = (1-p_d^{\mathcal{X}})\sum_{\beta=0}^{\infty}(1-\eta_r\eta_l)^{\beta}\,\mathrm{Tr}\left[\bar{\sigma}\,\Pi^{0}_{\mathcal{Z}}\Pi^{\beta}_{\mathcal{X}}\Pi^{0}_{\mathcal{Z}}\right] \tag{C140}$$

and the equation for the case $\alpha = 1$ as

$$\mathrm{Tr}[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}] - \left[\eta_l \mathbb{Y}^{1t}_{\eta_l} + (1-\eta_l)\mathbb{Y}^{1r}_{\eta_l}\right] = (1-p_d^{\mathcal{X}}) \sum_{\beta=0}^{\infty} (1-\eta_r\eta_l)^{\beta}\, \mathrm{Tr}\left[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}\Pi^{\beta}_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right], \tag{C141}$$

where $\mathrm{Tr}[\bar{\sigma}\,\Pi^{\alpha}_{\mathcal{Z}}]$ is bounded from above and below in Eqs. (B6)–(B9), while $\mathbb{Y}^{0}_{\eta_l}$, $\mathbb{Y}^{1t}_{\eta_l}$, and $\mathbb{Y}^{1r}_{\eta_l}$ are bounded in Eqs. (B12)–(B17). This allows us to consider the left-hand sides in Eqs. (C140) and (C141) as known quantities, thus enabling us to perform the detector decoy technique independently on the two equations, as illustrated in Appendix C 4 k. In this way, we are able to obtain accurate upper bounds on $\mathrm{Tr}\left[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^0_{\mathcal{Z}}\right]$ and $\mathrm{Tr}\left[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right]$ in terms of observed statistics:

$$\mathrm{Tr}\left[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^0_{\mathcal{Z}}\right] \leq \overline{\left[w^0_{\mathcal{X}}\right]^0_{\mathcal{Z}}} \tag{C142}$$

and

$$\mathrm{Tr}\left[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right] \leq \overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}, \tag{C143}$$

where the explicit expressions for $\overline{\left[w^0_{\mathcal{X}}\right]^0_{\mathcal{Z}}}$ and $\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}$ are given in Eqs. (B10) and (B11).

After having obtained the upper bounds in Eqs. (C142) and (C143), we now focus on deriving an upper bound on the remaining expectation value in Eq. (C122), namely, $\mathrm{Tr}\left[\bar{\sigma}\,(\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}} + \mathrm{H.c.})\right]$. To this aim, we define

$$z := \mathrm{Tr}\left[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right] \tag{C144}$$

such that the expectation value of interest can be bounded as follows:

$$\begin{aligned}\mathrm{Tr}\left[\bar{\sigma}\,(\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}} + \mathrm{H.c.})\right] &= z + z^* \\ &= 2\mathrm{Re}(z) \\ &\leq 2|z| \\ &= 2\left|\mathrm{Tr}\left[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right]\right|.\end{aligned} \tag{C145}$$

We can use the Cauchy-Schwarz inequality in the following form:

$$\left|\mathrm{Tr}[A^\dagger B]\right| \leq \sqrt{\mathrm{Tr}[A^\dagger A]\,\mathrm{Tr}[B^\dagger B]}, \tag{C146}$$

where we choose $A = \sqrt{\bar{\sigma}}$ and $B = \Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\sqrt{\bar{\sigma}}$. We obtain

$$\begin{aligned}\mathrm{Tr}\left[\bar{\sigma}\,(\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}} + \mathrm{H.c.})\right] &\leq 2\sqrt{\mathrm{Tr}\left[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right]} \\ &\leq 2\sqrt{\mathrm{Tr}\left[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right]},\end{aligned} \tag{C147}$$

where we used the fact that $\Pi^0_{\mathcal{Z}} \leq \mathbb{1}$. Finally, we use the bound already established in Eq. (C143) and obtain the bound on the remaining expectation value:

$$\mathrm{Tr}\left[\bar{\sigma}\,(\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}} + \mathrm{H.c.})\right] \leq 2\left(\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}\right)^{\frac{1}{2}}, \tag{C148}$$

where $\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}$ is given in Eq. (B11).

By combining Eqs. (C142), (C143), and (C148) with Eq. (C122), we obtain an upper bound on the second term in Eq. (C103):

$$\begin{aligned}\mathrm{Tr}\left[\bar{\sigma} M^{\leq 1}_{\mathcal{Z}}\Pi^0_{\mathcal{X}}M^{\leq 1}_{\mathcal{Z}}\right] \leq\; & p_{\checkmark|0}\overline{\left[w^0_{\mathcal{X}}\right]^0_{\mathcal{Z}}} + p_{\checkmark|1}\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}} \\ & + 2\sqrt{p_{\checkmark|0}p_{\checkmark|1}}\left(\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}\right)^{\frac{1}{2}},\end{aligned} \tag{C149}$$

which is given in terms of observed statistics.

Finally, we use the results in Eqs. (C121) and (C149) in Eq. (C103), which provides us with the following upper bound on the phase error rate [see Eq. (C437) in Appendix C 4 m]:

$$\tilde{e}_{X,1} \leq \overline{\tilde{e}_{X,1}}, \tag{C150}$$

where

$$\begin{aligned}\overline{\tilde{e}_{X,1}} =\; & \frac{1}{\underline{Y^{\mathcal{Z}}_{1,(\eta_\downarrow,\eta_\downarrow)}}[p_d^{\mathcal{X}} + \eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})]}\left[p_{\checkmark|0}\overline{\mathbb{E}}^0_{\eta_\uparrow} + \sqrt{p_{\checkmark|0}p_{\checkmark|1}}\sqrt{\eta_\uparrow}\overline{\mathbb{E}}^{0,1}_{\eta_\uparrow} + p_{\checkmark|1}\left(\eta_\uparrow\overline{\mathbb{E}}^{1t}_{\eta_\uparrow} + (1-\eta_\uparrow)\overline{\mathbb{E}}^{1r}_{\eta_\uparrow}\right)\right] \\ & + \frac{\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}{\underline{Y^{\mathcal{Z}}_{1,(\eta_\downarrow,\eta_\downarrow)}}[p_d^{\mathcal{X}} + \eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})]}\left[p_{\checkmark|0}\overline{\left[w^0_{\mathcal{X}}\right]^0_{\mathcal{Z}}} + 2\sqrt{p_{\checkmark|0}p_{\checkmark|1}}\left(\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}\right)^{\frac{1}{2}} + p_{\checkmark|1}\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}\right] \\ & + \frac{1}{\underline{Y^{\mathcal{Z}}_{1,(\eta_\downarrow,\eta_\downarrow)}}}\left(\overline{\Delta_2} + \overline{w}^{>1}_{\mathcal{Z}}\right),\end{aligned} \tag{C151}$$

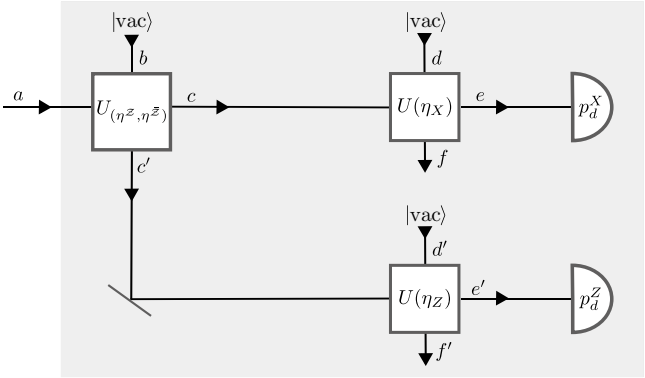


FIG. 6. Bob's measurement apparatus. In each round, the incoming signal (mode $a$) enters a TBS described by the unitary $U_{(\eta_i,\eta_l)}$, where $(\eta_i,\eta_l)$ is the TBS setting for that particular round. The transmitted mode (mode $c$) is detected by an $X$-basis detector with efficiency $\eta_X$ and dark count probability $p_d^X$ for each outcome. This is modeled by a beam splitter $[U(\eta_X)]$ followed by a perfect detector with dark count probability $p_d^X$. The reflected mode (mode $c'$) is detected by a $Z$-basis detector with efficiency $\eta_Z$ and dark count probability $p_d^{Z_X}$ per outcome, which is similarly modeled. Note that the insertion loss of the TBS is accounted for in the efficiencies of the two detectors.

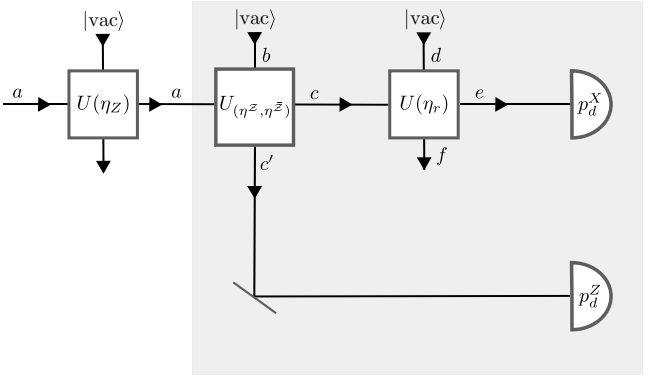


FIG. 7. Bob's simplified measurement apparatus. Here the common loss of the two detectors in Fig. 6—which amounts to $1-\eta_Z$—has been factored outside Bob's apparatus, leaving an ideal detector in the $Z$ basis and a lossy detector in the $X$ basis with efficiency $\eta_r=\eta_X/\eta_Z$.

and where we replaced the one-photon $Z$-basis yield with the corresponding lower bound from the decoy-state method. We emphasize that all the quantities appearing in Eq. (C151) are either known or obtained with the decoy-state method (see Appendix D for the formulas for the decoy-state method). This concludes the derivation of a computable upper bound on the phase error rate.

### *b. Bob's measurement apparatus*

We now detail the missing steps of the argument. The method that we introduce to estimate the phase error rate relies on a partial characterization of Bob's measurement apparatus, as described in Sec. III. In Fig. 6, we provide a model of Bob's measurement apparatus. Here, the nonunit detection efficiency of the $Z$-basis detector ($X$-basis detector) is modeled by a beam splitter with transmittance $\eta_Z$ ($\eta_X$), described by the unitary $U(\eta_Z)$ $[U(\eta_X)]$. The TBS is described by a unitary $U_{(\eta_i,\eta_l)}$ acting on spatial-temporal modes $a_t^\dagger$ and $b_t^\dagger$ as follows:

$$U_{(\eta_i,\eta_l)}=\begin{cases}U(\eta_i) & \text{if } t\in\mathcal{Z},\\ U(\eta_l) & \text{if } t\notin\mathcal{Z},\end{cases} \tag{C152}$$

where $\mathcal{Z}=\sum_{j=0}^{d-1}\mathcal{Z}_j$ is the union of all the modes that are detected by the $Z$-basis detector. In the case where the $Z$-basis detection is a time-of-arrival measurement, $\mathcal{Z}$ corresponds to the union of all the time bins. We recall that, in each round, Bob selects one of the following six TBS settings: $(\eta_i,\eta_\uparrow)$ and $(\eta_i,\eta_\downarrow)$, with $\eta_1=\eta_\uparrow$, $\eta_3=\eta_\downarrow$, and $\eta_2$ satisfying $\eta_\downarrow<\eta_2<\eta_\uparrow$. Moreover, we recall that the TBS settings and the detection efficiencies of the two detectors must satisfy Eqs. (9) and (10).

In our formalism, the unitary $U(\eta)$ maps the input modes $\mathrm{m}_1^\dagger=a^\dagger,c^\dagger,c'^\dagger$ and $\mathrm{m}_2^\dagger=b^\dagger,d^\dagger,d'^\dagger$ to the output modes $\mathrm{M}_1^\dagger=c^\dagger,e^\dagger,e'^\dagger$ and $\mathrm{M}_2^\dagger=c'^\dagger,f^\dagger,f'^\dagger$, respectively, as follows:

$$\begin{pmatrix}\mathrm{M}_1^\dagger\\ \mathrm{M}_2^\dagger\end{pmatrix}=U(\eta)\begin{pmatrix}\mathrm{m}_1^\dagger\\ \mathrm{m}_2^\dagger\end{pmatrix},$$
$$\text{with}\quad U(\eta):=\begin{pmatrix}\sqrt{\eta} & -\sqrt{1-\eta}\\ \sqrt{1-\eta} & \sqrt{\eta}\end{pmatrix}. \tag{C153}$$

We simplify Bob's measurement apparatus. The idea is to factor out the common loss in the two detectors and view it as loss occurring in the channel from Alice to Bob, before it reaches Bob's measurement apparatus. More specifically, we define the ratio between the efficiency of the $X$-basis detector and the efficiency of the $Z$-basis detector:

$$\eta_r:=\frac{\eta_X}{\eta_Z}, \tag{C154}$$

where we have $0<\eta_r<1$ since we assumed in Sec. III that the detector used to generate key bits is more efficient. This is a sensible assumption that typically leads to better key rates; however, if not verified, one can always exchange the roles of the two bases. Then, we can re-express the efficiency of the $X$-basis detector as $\eta_X=\eta_Z\eta_r$, which allows us to factor out the transmittance that is shared by the two detectors, namely, $\eta_Z$. In particular, we can equivalently describe Bob's apparatus as depicted in Fig. 7, where we introduced a beam splitter with transmittance $\eta_Z$ before Bob's apparatus, which accounts for the common loss of both detectors, and replaced the $Z$-basis

detector ($X$-basis detector) detector with a lossless detector (lossy detector with efficiency $\eta_r$). This equivalence is well known in quantum optics; see, e.g., Ref. [56].

Furthermore, we argue that it can be advantageous to Eve only if we give her control over the beam splitter preceding Bob's apparatus [$U(\eta_Z)$] by viewing it as part of the insecure channel between Alice and Bob. Therefore, from now on, we ignore the unitary $U(\eta_Z)$ and describe Bob's apparatus as depicted in Fig. 7.

### *c. Bob's Z-basis detector*

The next step of the proof consists of a reduction of the phase error rate to the subspace with at most one photon in the interval $\mathcal{Z}$, which we call the "($\leq 1$)-subspace" for brevity. Intuitively, this is the subspace where most of the states in $\{\sigma_k\}_k$ should lie in the absence of an eavesdropper.

*Remark 3.* We recall that $\sigma_k$ is the state received by Bob when Alice encodes the test symbol $X_A = k$ on a single photon. However, since we do not restrict Eve's collective attack, we cannot assume that the states $\{\sigma_k\}_k$ are confined to, for example, the subspace with at most one photon. Eve could perform attacks where she adds photons to the states sent by Alice. This could allow her to control the click probability of the two bases if they have asymmetric detection efficiencies. We emphasize that while previous analytical QKD proofs are restricted to the one-photon subspace when dealing with detection efficiency mismatches [11,33,34], our proof can accommodate both mode-dependent and mode-independent mismatches in the detection probability without posing any constraint on the states received by Bob.

Because, as argued in Remark C3, we do not constrain the states $\sigma_k$, we are forced to estimate their weight in the ($\leq 1$)-subspace, enabling us to reduce the calculation of the phase error rate to the ($\leq 1$)-subspace.

The estimation of the states' weight in the ($\leq 1$)-subspace is done from the statistics of the $Z$-basis detector. Thus, as the first step, we derive an explicit expression for some of the elements of the POVM $\{(Z_0)_{c'}, (Z_1)_{c'}, \ldots, (Z_{d-1})_{c'}, (Z_\emptyset)_{c'}\}$ that describes Bob's $Z$-basis measurement in the reflected mode of the TBS, where the subscript indicates the spatial mode on which the operator acts (see Fig. 7).

Let $\Pi^\alpha_{\mathcal{Z}}$ be the projector of $n = \alpha$ photons in the global detection interval $\mathcal{Z}$, while acting as the identity outside the interval $\mathcal{Z}$. Then the POVM element corresponding to a detection of one of the $d$ outcomes would be $(Z_\checkmark)_{c'} = \sum_{j=0}^{d-1}(Z_j)_{c'} = \sum_{\alpha=1}^{\infty}(\Pi^\alpha_{\mathcal{Z}})_{c'}$ in the absence of dark counts, i.e., the projector in the subspace with at least one photon in $\mathcal{Z}$. Note that this is true since we assumed that multiclick events are always mapped to a single outcome (see Sec. III). However, since the detector has a dark count probability $p_d^Z$ per outcome, the POVM element corresponding to a detection becomes

$$(Z_\checkmark)_{c'} := p_d^{\mathcal{Z}}\left[\mathbb{1} - \sum_{\alpha=1}^{\infty}\Pi^\alpha_{\mathcal{Z}}\right] + \sum_{\alpha=1}^{\infty}\Pi^\alpha_{\mathcal{Z}} = p_d^{\mathcal{Z}}\mathbb{1} + (1-p_d^{\mathcal{Z}})\sum_{\alpha=1}^{\infty}\Pi^\alpha_{\mathcal{Z}}, \tag{C155}$$

where $p_d^{\mathcal{Z}}$ is defined in Eq. (B2). Note that if the $Z$-basis detector implemented a time-of-arrival measurement, the projector $\Pi^\alpha_{\mathcal{Z}}$ would be given by

$$\Pi^\alpha_{\mathcal{Z}} = \sum_{n=\alpha}^{\infty}\Pi^\alpha_{\mathcal{Z},n}, \tag{C156}$$

where $\Pi^\alpha_{\mathcal{Z},n}$ is the projector on the subspace of $n$ photons, with exactly $\alpha$ photons localized in the time interval $\mathcal{Z}$:

$$\Pi^\alpha_{\mathcal{Z},n} = \int_{\mathcal{Z}}\frac{\mathrm{d}t_1\cdots\mathrm{d}t_\alpha}{\alpha!} \times \int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t_{\alpha+1}\cdots\mathrm{d}t_n}{(n-\alpha)!}|1_{t_1},\ldots,1_{t_n}\rangle\langle 1_{t_1},\ldots,1_{t_n}|, \tag{C157}$$

where $\overline{\mathcal{Z}}$ is the complement of $\mathcal{Z}$ in the time domain and $|1_t\rangle = a_t^\dagger|\mathrm{vac}\rangle$ represents the unphysical state of one photon at time $t$. We have that $a_t^\dagger$ creates a photon at time $t$ as the Fourier transform of a photon with frequency $f$ :

$$a_t^\dagger = \int_{-\infty}^{\infty}\mathrm{d}f e^{2\pi i f t}a_f^\dagger. \tag{C158}$$

Moreover, it holds that $[a_t^\dagger, a_{t'}^\dagger] = 0$ and $[a_t, a_{t'}^\dagger] = \delta(t-t')\mathbb{1}$, which implies

$$\langle 1_{t_1},\ldots,1_{t_n}|1_{t'_1},\ldots,1_{t'_k}\rangle = \delta_{n,k}\sum_{\pi\in S_n}\delta(t_1-t'_{\pi(1)})\ldots\delta(t_n-t'_{\pi(n)}), \tag{C159}$$

where $S_n$ is the set of all permutations of indexes in $\{1,2,\ldots,n\}$. To familiarize ourselves with this formalism, which allows $n$ photons to be arbitrarily delocalized in time, we can verify that

$$\sum_{\alpha=0}^{\infty}\Pi^\alpha_{\mathcal{Z}} = \mathbb{1} \tag{C160}$$

holds. The following proof is not essential to the remainder of this appendix and can be skipped.

*Proof of Eq. (C160).* By using Eq. (C156), we can rewrite the sum over $\alpha$ as follows:

$$\sum_{\alpha=0}^{\infty}\Pi_{\mathcal{Z}}^{\alpha}=\sum_{\alpha=0}^{\infty}\sum_{n=\alpha}^{\infty}\Pi_{\mathcal{Z},n}^{\alpha}=\sum_{n=0}^{\infty}\sum_{\alpha=0}^{n}\Pi_{\mathcal{Z},n}^{\alpha}. \tag{C161}$$

By comparing the last expression with

$$\mathbb{1}=\sum_{n=0}^{\infty}\Pi_n, \tag{C162}$$

where $\Pi_n$ is the projector on the subspace of $n$ photons

$$\Pi_n=\int_{-\infty}^{\infty}\frac{\mathrm{d}t_1\cdots\mathrm{d}t_n}{n!}|1_{t_1},\ldots,1_{t_n}\rangle\langle 1_{t_1},\ldots,1_{t_n}|, \tag{C163}$$

we are left to prove that $\Pi_n=\sum_{\alpha=0}^{n}\Pi_{\mathcal{Z},n}^{\alpha}$, i.e., that

$$\begin{aligned}&\int_{-\infty}^{\infty}\frac{\mathrm{d}t_1\cdots\mathrm{d}t_n}{n!}|1_{t_1},\ldots,1_{t_n}\rangle\langle 1_{t_1},\ldots,1_{t_n}|\\&=\sum_{\alpha=0}^{n}\int_{\mathcal{Z}}\frac{\mathrm{d}t_1\cdots\mathrm{d}t_\alpha}{\alpha!}\\&\quad\times\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t_{\alpha+1}\cdots\mathrm{d}t_n}{(n-\alpha)!}|1_{t_1},\ldots,1_{t_n}\rangle\langle 1_{t_1},\ldots,1_{t_n}|.\end{aligned} \tag{C164}$$

To prove Eq. (C164), we independently apply the left-hand side and right-hand side on a generic state and verify that the resulting states coincide. Let $|\Psi\rangle$ be an $n$-photon state defined as

$$|\Psi\rangle=\int_{-\infty}^{\infty}\mathrm{d}\tau_1\cdots\mathrm{d}\tau_n f(\tau_1,\ldots,\tau_n)\,|1_{\tau_1},\ldots,1_{\tau_n}\rangle, \tag{C165}$$

where $f(\tau_1,\ldots,\tau_n)$ is an arbitrary time distribution function. We have

$$\begin{aligned}\Pi_n|\Psi\rangle&=\int_{-\infty}^{\infty}\frac{\mathrm{d}t_1\cdots\mathrm{d}t_n}{n!}|1_{t_1},\ldots,1_{t_n}\rangle\sum_{\pi\in S_n}f(t_{\pi(1)},\ldots,t_{\pi(n)})\\&=\int_{-\infty}^{\infty}\mathrm{d}t_1\cdots\mathrm{d}t_n f(t_1,\ldots,t_n)\,|1_{t_1},\ldots,1_{t_n}\rangle=|\Psi\rangle,\end{aligned} \tag{C166}$$

where we used Eq. (C159) in the first equality and renamed $t_{\pi(1)}\to t_1,\ldots,t_{\pi(n)}\to t_n$ in the second equality. Now we compute

$$\begin{aligned}&\sum_{\alpha=0}^{n}\Pi_{\mathcal{Z},n}^{\alpha}|\Psi\rangle\\&=\sum_{\alpha=0}^{n}\int_{\mathcal{Z}}\frac{\mathrm{d}t_1\cdots\mathrm{d}t_\alpha}{\alpha!}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t_{\alpha+1}\cdots\mathrm{d}t_n}{(n-\alpha)!}|1_{t_1},\ldots,1_{t_n}\rangle\\&\quad\times\sum_{\pi\in S_n}f(t_{\pi(1)},\ldots,t_{\pi(n)})\\&=\sum_{\alpha=0}^{n}\sum_{\pi\in S_n}\int_{\mathcal{Z}}\frac{\mathrm{d}t_{\pi(1)}\cdots\mathrm{d}t_{\pi(\alpha)}}{\alpha!}\\&\quad\times\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t_{\pi(\alpha+1)}\cdots\mathrm{d}t_{\pi(n)}}{(n-\alpha)!}|1_{t_1},\ldots,1_{t_n}\rangle f(t_1,\ldots,t_n),\end{aligned} \tag{C167}$$

where we renamed $t_{\pi(1)}\to t_1,\ldots,t_{\pi(n)}\to t_n$ in the second equality. Note that $|1_{t_1}\ldots 1_{t_n}\rangle$ remains unchanged because it is permutationally invariant. Now we observe that the following equality holds after expanding the left-hand side:

$$\begin{aligned}&\left(\int_{\mathcal{Z}}\mathrm{d}t_1+\int_{\overline{\mathcal{Z}}}\mathrm{d}t_1\right)\cdots\left(\int_{\mathcal{Z}}\mathrm{d}t_n+\int_{\overline{\mathcal{Z}}}\mathrm{d}t_n\right)\\&=\sum_{\alpha=0}^{n}\sum_{\pi\in S_n}\int_{\mathcal{Z}}\frac{\mathrm{d}t_{\pi(1)}\cdots\mathrm{d}t_{\pi(\alpha)}}{\alpha!}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t_{\pi(\alpha+1)}\cdots\mathrm{d}t_{\pi(n)}}{(n-\alpha)!},\end{aligned} \tag{C168}$$

where the division by $\alpha!$ and $(n-\alpha)!$ ensures that the permutations where the only terms permuting are within the same integration range are not counted more than once. Then, by combining the previous equality with

$$\left(\int_{\mathcal{Z}}\mathrm{d}t_1+\int_{\overline{\mathcal{Z}}}\mathrm{d}t_1\right)\cdots\left(\int_{\mathcal{Z}}\mathrm{d}t_n+\int_{\overline{\mathcal{Z}}}\mathrm{d}t_n\right)=\int_{-\infty}^{\infty}\mathrm{d}t_1\cdots\mathrm{d}t_n \tag{C169}$$

and using this in Eq. (C168), we obtain

$$\begin{aligned}&\sum_{\alpha=0}^{n}\Pi_{\mathcal{Z},n}^{\alpha}|\Psi\rangle\\&=\int_{-\infty}^{\infty}\mathrm{d}t_1\cdots\mathrm{d}t_n f(t_1,\ldots,t_n)\,|1_{t_1},\ldots,1_{t_n}\rangle=|\Psi\rangle,\end{aligned} \tag{C170}$$

which proves Eq. (C164) and thus concludes the proof. ■

*Remark 4.* Note that if Bob's $Z$-basis measurement corresponds to measuring a different degree of freedom than the arrival time of the signal, one can still use Eqs. (C155)

and (C156) for other degrees of freedom, while the time degree of freedom should be replaced by the measured degree of freedom in Eq. (C157).

We have thus obtained the expression (C155) for the POVM element representing a detection in the $Z$-basis detector, acting on the reflected mode $c'$. However, the actual measurement statistics are collected from Bob's global measurement on the received signal (mode $a$), which comprises detections in both the $Z$-basis detector and the $X$-basis detector and is formally introduced in Eq. (C6). Nevertheless, similarly to Eq. (C7), from the global POVM (C6) we can define a POVM element on mode $a$ that corresponds to a detection in the $Z$ detector and ignores the outcome of the $X$-basis detector:

$$Z_{\checkmark}^{(\eta_l,\eta_l)} := \sum_{j=0}^{d-1} M_{j,\emptyset}^{(\eta_l,\eta_l)} + \sum_{j,k=0}^{d-1} M_{j,k}^{(\eta_l,\eta_l)}, \tag{C171}$$

where the superscript indicates the TBS setting. Note that $Z_{\checkmark}^{(\eta_\downarrow,\eta_\downarrow)} = Z_{\checkmark}$, where $Z_{\checkmark}$ is the POVM element for a detection in Bob's key generation measurement and it appears in the phase error rate.

To obtain an explicit expression for $Z_{\checkmark}^{(\eta_l,\eta_l)}$, we first note that the one-photon $Z$-basis yield with TBS setting $(\eta_l, \eta_l)$ is, similarly to Eq. (C51), given by

$$\begin{aligned} &Y^Z_{1,(\eta_l,\eta_l)} \\ &= \sum_{j=0}^{d-1} \frac{1}{d} \Pr(Z_B \neq \emptyset | T = Z, N_A = 1, Z_A = j, (\eta_l, \eta_l)) \\ &= \sum_{j=0}^{d-1} \frac{1}{d} \operatorname{Tr}\Big[ (Z_{\checkmark}^{(\eta_l,\eta_l)} \otimes \mathbb{1}_E) U_{BE} |1_{Z_j}\rangle\langle 1_{Z_j}|_B \\ &\quad \otimes |0\rangle\langle 0|_E U_{BE}^\dagger \Big] \\ &= \operatorname{Tr}_a \left[ \bar{\sigma} Z_{\checkmark}^{(\eta_l,\eta_l)} \right], \end{aligned} \tag{C172}$$

where in the second equality we used a generalization of Eq. (C39) and in the third equality the fact that Eq. (7) holds, together with a shorthand notation for the average state received by Bob:

$$\bar{\sigma} := \frac{1}{d} \sum_{k=0}^{d-1} \sigma_k, \tag{C173}$$

with $\sigma_k$ given in Eq. (C74). At the same time, by using the scheme in Fig. 7 and the definition of the TBS unitary in Eq. (C152), we have

$$\begin{aligned} &Y^Z_{1,(\eta_l,\eta_l)} \\ &= \operatorname{Tr}_{cc'} \left[ U(\eta_l) \bar{\sigma}_a \otimes |\mathrm{vac}\rangle\langle \mathrm{vac}|_b U(\eta_l)^\dagger \mathbb{1}_c \otimes (Z_{\checkmark})_{c'} \right] \\ &= \operatorname{Tr}_{ab} \left[ \bar{\sigma}_a \otimes |\mathrm{vac}\rangle\langle \mathrm{vac}|_b U(\eta_l)^\dagger \mathbb{1}_c \otimes (Z_{\checkmark})_{c'} U(\eta_l) \right] \\ &= \operatorname{Tr}_a \left[ \bar{\sigma}_a \langle \mathrm{vac}|_b U(\eta_l)^\dagger \mathbb{1}_c \otimes (Z_{\checkmark})_{c'} U(\eta_l) |\mathrm{vac}\rangle_b \right]. \end{aligned} \tag{C174}$$

By comparing Eqs. (C172) and (C174), we deduce an expression for the operator in Eq. (C171):

$$\begin{aligned} Z_{\checkmark}^{(\eta_l,\eta_l)} &= \langle \mathrm{vac}|_b U(\eta_l)^\dagger \mathbb{1}_c \otimes (Z_{\checkmark})_{c'} U(\eta_l) |\mathrm{vac}\rangle_b \\ &= p_d^{\mathcal{Z}} \mathbb{1} + (1 - p_d^{\mathcal{Z}}) \langle \mathrm{vac}|_b U(\eta_l)^\dagger \mathbb{1}_c \\ &\quad \otimes \sum_{\alpha=1}^{\infty} (\Pi_{\mathcal{Z}}^{\alpha})_{c'} U(\eta_l) |\mathrm{vac}\rangle_b, \end{aligned} \tag{C175}$$

where in the second equality we used Eq. (C155). We now define the following operator acting on mode $a$:

$$Q := \langle \mathrm{vac}|_b U(\eta_l)^\dagger \mathbb{1}_c \otimes \sum_{\alpha=1}^{\infty} (\Pi_{\mathcal{Z}}^{\alpha})_{c'} U(\eta_l) |\mathrm{vac}\rangle_b. \tag{C176}$$

We can explicitly calculate $Q$ by applying the unitary $U(\eta_l)$ according to Eq. (C153). To do so, we make $(\Pi_{\mathcal{Z}}^{\alpha})_{c'}$ and $\mathbb{1}_c$ explicit according to Eqs. (C156), (C157), and (C160). Then, by linearity, we obtain some terms like the following:

$$\begin{aligned} &\langle \mathrm{vac}|_b U^\dagger(\eta_l) c_{t_1}^\dagger \dots c_{t_n}^\dagger (c')_{t'_1}^\dagger \dots (c')_{t'_m}^\dagger |\mathrm{vac}\rangle \\ &\quad \times \langle \mathrm{vac}| c_{t_1} \dots c_{t_n} (c')_{t'_1} \dots (c')_{t'_m} U(\eta_l) |\mathrm{vac}\rangle_b \\ &= \eta_l^n (1 - \eta_l)^m |1_{t_1}, \dots, 1_{t_n}, 1_{t'_1}, \dots, 1_{t'_m}\rangle \\ &\quad \times \langle 1_{t_1}, \dots, 1_{t_n}, 1_{t'_1}, \dots, 1_{t'_m}|_a, \end{aligned} \tag{C177}$$

which corresponds to a pure state on mode $a$. By using Eq. (C177) in Eq. (C176) and by reparametrizing the resulting sums, we obtain

$$Q = \sum_{\alpha=1}^{\infty} (1 - \eta_l^\alpha) (\Pi_{\mathcal{Z}}^{\alpha})_a. \tag{C178}$$

By using this expression in Eq. (C175), we find the final expression for the POVM element (C171) describing a detection in the $Z$-basis detector with the TBS setting

$(\eta_l, \eta_l)$:

$$Z_{\checkmark}^{(\eta_l,\eta_l)} = p_d^{\mathcal{Z}} \mathbb{1} + (1-p_d^{\mathcal{Z}}) \sum_{\alpha=1}^{\infty} (1-\eta_l^{\alpha}) \Pi_{\mathcal{Z}}^{\alpha}$$
$$= \sum_{\alpha=0}^{\infty} \left[1-(1-p_d^{\mathcal{Z}})\eta_l^{\alpha}\right] \Pi_{\mathcal{Z}}^{\alpha}. \tag{C179}$$

This operator has a twofold purpose. First, by recalling the definition of Bob's key generation measurement in Eq. (C7), it provides us with the explicit expression for the operator $Z_{\checkmark}$ that appears in the phase error rate formula (C94):

$$Z_{\checkmark} = Z_{\checkmark}^{(\eta_{\downarrow},\eta_{\downarrow})}$$
$$= \sum_{\alpha=0}^{\infty} p_{\checkmark|\alpha} \Pi_{\mathcal{Z}}^{\alpha}, \tag{C180}$$

where we identified $p_{\checkmark|\alpha}$ as the probability of a detection in the $Z$-basis detector, given that the state received by Bob contains $\alpha$ photons localized in the detection interval $\mathcal{Z}$,

$$p_{\checkmark|\alpha} := 1-(1-p_d^{\mathcal{Z}})\eta_{\downarrow}^{\alpha}. \tag{C181}$$

We also specify the above expression for the cases $\alpha = 0$ and $\alpha = 1$:

$$p_{\checkmark|0} = p_d^{\mathcal{Z}}, \tag{C182}$$
$$p_{\checkmark|1} = 1-(1-p_d^{\mathcal{Z}})\eta_{\downarrow}. \tag{C183}$$

Secondly, the operator in Eq. (C179) allows us to estimate the weight of the states received by Bob in the $(\leq 1)$-subspace, through the detector decoy technique [28].

### *d. The detector decoy technique applied on the Z-basis detector statistics*

The detector decoy technique [28] is a powerful tool that allows one to estimate the weight of measured states in various subspaces with a fixed photon number. In our case, for the purpose of reducing the phase error rate calculation to the $(\leq 1)$-subspace, we are interested in estimating the weight of the average state received by Bob in the subspaces defined by $\Pi_{\mathcal{Z}}^0$ and $\Pi_{\mathcal{Z}}^1$. More precisely, let

$$\mathrm{Tr}\left[\bar{\sigma}\,\Pi_{\mathcal{Z}}^{\alpha}\right] \text{ for } \alpha = 0, 1, \ldots, \infty \tag{C184}$$

be the weight of $\bar{\sigma}$ in the subspace with $\alpha$ photons localized in $\mathcal{Z}$. Then the goal is to derive upper and lower bounds on $\mathrm{Tr}[\bar{\sigma}\,\Pi_{\mathcal{Z}}^0]$ and $\mathrm{Tr}[\bar{\sigma}\,\Pi_{\mathcal{Z}}^1]$.

To this aim, we will use the statistics of the no-detection events in the $Z$-basis detector with TBS setting $(\eta_l, \eta_l)$, which are generated by the following POVM element:

$$Z_{\emptyset}^{(\eta_l,\eta_l)} = \mathbb{1} - Z_{\checkmark}^{(\eta_l,\eta_l)}$$
$$= (1-p_d^{\mathcal{Z}}) \sum_{\alpha=0}^{\infty} \eta_l^{\alpha} \Pi_{\mathcal{Z}}^{\alpha}, \tag{C185}$$

where we used Eq. (C179). Therefore, the probability of no detection in the $Z$-basis detector reads

$$1 - Y_{1,(\eta_l,\eta_l)}^{Z} = \mathrm{Tr}\left[\bar{\sigma} Z_{\emptyset}^{(\eta_l,\eta_l)}\right]$$
$$= (1-p_d^{\mathcal{Z}}) \sum_{\alpha=0}^{\infty} \eta_l^{\alpha}\, \mathrm{Tr}[\bar{\sigma}\,\Pi_{\mathcal{Z}}^{\alpha}]. \tag{C186}$$

The detector decoy technique is based on a set of equations of the following form:

$$f_l = \sum_{\alpha=0}^{\infty} \eta_l^{\alpha} y_{\alpha}, \tag{C187}$$

where $f_l$ are known quantities that are experimentally observed, $y_{\alpha} \in [0,1]$ are the variables that are to be bounded, and $\eta_l$ is a parameter that can be fixed to different values by one varying $l$. In our case, Eq. (C186) can be put in the form of Eq. (C187) by one identifying

$$f_l = \frac{1 - Y_{1,(\eta_l,\eta_l)}^{Z}}{1-p_d^{\mathcal{Z}}}, \tag{C188}$$
$$y_{\alpha} = \mathrm{Tr}[\bar{\sigma}\,\Pi_{\mathcal{Z}}^{\alpha}], \tag{C189}$$

from which we deduce the normalization property of the variables $\{y_{\alpha}\}_{\alpha}$:

$$\textstyle\sum_{\alpha=0}^{\infty} y_{\alpha} = 1. \tag{C190}$$

We now apply the idea of the detector decoy technique to Eq. (C187) to derive an upper bound and a lower bound on $y_0$ and $y_1$. We recall that among Bob's possible choices for the TBS setting (see Sec. III), we have $\eta_1 = \eta_{\uparrow}$ and $\eta_3 = \eta_{\downarrow}$.

We start by deriving the upper bound on $y_0$. Consider the following system of two inequalities, obtained from Eqs. (C187) and (C190):

$$
\begin{aligned}
&\begin{cases} f_1 \leq y_0 + \eta_1 y_1 + \eta_1^2(1 - y_0 - y_1), \\ f_3 \geq y_0 + \eta_3 y_1 \end{cases} \\
\Rightarrow \quad &\begin{cases} y_1 \geq \frac{f_1 - y_0 - \eta_1^2(1-y_0)}{\eta_1(1-\eta_1)}, \\ y_0 + \eta_3 \frac{f_1 - y_0 - \eta_1^2(1-y_0)}{\eta_1(1-\eta_1)} \leq f_3 \end{cases} \\
\Rightarrow \quad &\begin{cases} y_1 \geq \frac{f_1 - y_0 - \eta_1^2(1-y_0)}{\eta_1(1-\eta_1)}, \\ y_0 \left[1 - \eta_3 \frac{1+\eta_1}{\eta_1}\right] \leq f_3 - \eta_3 \frac{f_1}{\eta_1(1-\eta_1)} + \frac{\eta_1 \eta_3}{1-\eta_1}, \end{cases}
\end{aligned} \tag{C191}
$$

where in the second step we used the lower bound on $y_1$ in the second inequality. From the bottom inequality in Eq. (C191), we can derive an upper bound on $y_0$, provided that its coefficient is positive. We thus require that

$$
\begin{aligned}
&\eta_1 - \eta_3(1 + \eta_1) > 0 \\
\iff \quad &\eta_\uparrow > \frac{\eta_\downarrow}{1 - \eta_\downarrow},
\end{aligned} \tag{C192}
$$

which is indeed satisfied since we assumed that the condition in Eq. (9) holds. Then the upper bound on $y_0$ can be derived from Eq. (C191) and reads

$$
y_0 \leq \frac{\eta_1 f_3 - \eta_3 f_1 + \eta_1^2(\eta_3 - f_3)}{(1 - \eta_1)\left[\eta_1 - \eta_3(1 + \eta_1)\right]}. \tag{C193}
$$

Finally, we substitute back the values for $\eta_1$, $\eta_3$, $f_l$, and $y_0$ and obtain the desired upper bound on the weight of the state in the subspace with no photon in $\mathcal{Z}$ in terms of observed quantities:

$$
\mathrm{Tr}[\tilde{\sigma}\, \Pi^0_{\mathcal{Z}}] \leq \overline{w}^0_{\mathcal{Z}}, \tag{C194}
$$

with

$$
\overline{w}^0_{\mathcal{Z}} := \min \left\{ 1, \frac{\overline{\eta_\downarrow Y^{\mathcal{Z}}_{1,(\eta_\uparrow,\eta_\uparrow)} - \eta_\uparrow(1-\eta_\uparrow) Y^{\mathcal{Z}}_{1,(\eta_\downarrow,\eta_\downarrow)}} + \eta_\uparrow(1-\eta_\uparrow) - \eta_\downarrow + \eta_\uparrow^2 \eta_\downarrow (1 - p_d^{\mathcal{Z}})}{(1 - p_d^{\mathcal{Z}})(1-\eta_\uparrow)\left[\eta_\uparrow - \eta_\downarrow(1+\eta_\uparrow)\right]} \right\}, \tag{C195}
$$

where we used the fact that $\Pi^0_{\mathcal{Z}} \leq \mathbb{1}$ to impose that $\overline{w}^0_{\mathcal{Z}} \leq 1$ and where we replaced the terms containing the yields $Y^{\mathcal{Z}}_{1,(\eta_l,\eta_l)}$—which are unobserved—with a bespoke upper bound obtained with the decoy-state method (see Appendix D), such that the resulting expression is still a valid upper bound.

Now we derive the upper bound on $y_1$. To this aim, we consider the following system of inequalities:

$$
\begin{aligned}
&\begin{cases} f_3 \leq y_0 + \eta_3 y_1 + \eta_3^2(1 - y_0 - y_1), \\ f_1 \geq y_0 + \eta_1 y_1 \end{cases} \\
\Rightarrow \quad &\begin{cases} y_0 \geq \frac{f_3 - y_1 \eta_3(1-\eta_3) - \eta_3^2}{1 - \eta_3^2}, \\ \frac{f_3 - y_1 \eta_3(1-\eta_3) - \eta_3^2}{1 - \eta_3^2} + \eta_1 y_1 \leq f_1 \end{cases} \\
\Rightarrow \quad &\begin{cases} y_0 \geq \frac{f_3 - y_1 \eta_3(1-\eta_3) - \eta_3^2}{1 - \eta_3^2}, \\ y_1 \left[\eta_1 - \frac{\eta_3}{1+\eta_3}\right] \leq f_1 - \frac{f_3}{1-\eta_3^2} + \frac{\eta_3^2}{1-\eta_3^2}, \end{cases}
\end{aligned} \tag{C196}
$$

where we used the lower bound on $y_0$ in the second inequality of the second step. From the bottom inequality in Eq. (C196), we can derive an upper bound on $y_1$, provided that its coefficient is positive, i.e., provided that

$$\eta_\uparrow > \frac{\eta_\downarrow}{1+\eta_\downarrow} \tag{C197}$$

holds, which is indeed the case since $\eta_\uparrow > \eta_\downarrow$. Then from Eq. (C196) we obtain the following upper bound on $y_1$:

$$y_1 \leq \frac{f_1 - f_3 + \eta_3^2(1-f_1)}{(1-\eta_3)\left[\eta_1(1+\eta_3)-\eta_3\right]}. \tag{C198}$$

In the original variables this becomes

$$\mathrm{Tr}[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}] \leq \overline{w}^1_{\mathcal{Z}}, \tag{C199}$$

with

$$\overline{w}^1_{\mathcal{Z}} := \min\left\{1, \frac{\overline{-(1-\eta_\downarrow^2)Y^Z_{1,(\eta_\uparrow,\eta_\uparrow)} + Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}} - \eta_\downarrow^2 p_d^{\mathcal{Z}}}{(1-p_d^{\mathcal{Z}})(1-\eta_\downarrow)\left[\eta_\uparrow(1+\eta_\downarrow)-\eta_\downarrow\right]}\right\}. \tag{C200}$$

We now turn to the derivation of the lower bounds on $y_0$ and $y_1$. The lower bound on $y_1$ can be obtained by one substituting the upper bound on $y_0$, Eq. (C193), into the lower bound on $y_1$ in Eq. (C191). By doing so and by simplifying the expression, we obtain

$$y_1 \geq \frac{f_1 - f_3 - \eta_1^2(1-f_3)}{(1-\eta_1)\left[\eta_1 - \eta_3(1+\eta_1)\right]}, \tag{C201}$$

which in the original variables becomes

$$\mathrm{Tr}[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}] \geq \underline{w}^1_{\mathcal{Z}}, \text{ with } \underline{w}^1_{\mathcal{Z}} := \max\left\{0, \frac{-\left(\overline{Y^Z_{1,(\eta_\uparrow,\eta_\uparrow)} - (1-\eta_\uparrow^2)Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}\right) + \eta_\uparrow^2 p_d^{\mathcal{Z}}}{(1-p_d^{\mathcal{Z}})(1-\eta_\uparrow)\left[\eta_\uparrow - \eta_\downarrow(1+\eta_\uparrow)\right]}\right\}. \tag{C202}$$

In a similar manner, we can substitute the upper bound on $y_1$, Eq. (C198), into the lower bound on $y_0$ from Eq. (C196). After some simplification, we obtain

$$y_0 \geq \frac{\eta_1 f_3 - \eta_3 f_1 - \eta_3^2(\eta_1 - f_1)}{(1-\eta_3)\left[\eta_1(1+\eta_3)-\eta_3\right]}, \tag{C203}$$

which in the original variables becomes

$$\mathrm{Tr}[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}] \geq \underline{w}^0_{\mathcal{Z}}, \text{ with:}$$
$$\underline{w}^0_{\mathcal{Z}} := \max\left\{0, \frac{-\left(\overline{-\eta_\downarrow(1-\eta_\downarrow)Y^Z_{1,(\eta_\uparrow,\eta_\uparrow)} + \eta_\uparrow Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}\right) + \eta_\uparrow - \eta_\downarrow(1-\eta_\downarrow) - \eta_\downarrow^2\eta_\uparrow(1-p_d^{\mathcal{Z}})}{(1-p_d^{\mathcal{Z}})(1-\eta_\downarrow)\left[\eta_\uparrow(1+\eta_\downarrow)-\eta_\downarrow\right]}\right\}. \tag{C204}$$

Finally, we derive the upper bound on the weight of the state $\bar{\sigma}$ in the subspaces with two or more photons localized in $\mathcal{Z}$. To this aim, we consider the following combination from Eq. (C187):

$$\begin{aligned} f_1 - \frac{\eta_1-\eta_3}{\eta_2-\eta_3} f_2 + \frac{\eta_1-\eta_2}{\eta_2-\eta_3} f_3 &= \sum_{\alpha=0}^{\infty} y_\alpha \left[ \eta_1^\alpha - \frac{\eta_1-\eta_3}{\eta_2-\eta_3}\eta_2^\alpha + \frac{\eta_1-\eta_2}{\eta_2-\eta_3}\eta_3^\alpha \right] \\ &= y_0 \left[ 1 - \frac{\eta_1-\eta_3}{\eta_2-\eta_3} + \frac{\eta_1-\eta_2}{\eta_2-\eta_3} \right] + y_1 \left[ \eta_1 - \frac{\eta_1-\eta_3}{\eta_2-\eta_3}\eta_2 + \frac{\eta_1-\eta_2}{\eta_2-\eta_3}\eta_3 \right] \\ &\quad + \sum_{\alpha=2}^{\infty} y_\alpha \left[ \eta_1^\alpha - \frac{\eta_1-\eta_3}{\eta_2-\eta_3}\eta_2^\alpha + \frac{\eta_1-\eta_2}{\eta_2-\eta_3}\eta_3^\alpha \right] \\ &= \sum_{\alpha=2}^{\infty} y_\alpha \frac{(\eta_2-\eta_3)\eta_1^\alpha - (\eta_1-\eta_3)\eta_2^\alpha + (\eta_1-\eta_2)\eta_3^\alpha}{\eta_2-\eta_3}, \end{aligned} \tag{C205}$$

from which we deduce

$$\begin{aligned} &(\eta_2-\eta_3)f_1 - (\eta_1-\eta_3)f_2 + (\eta_1-\eta_2)f_3 \\ &= \sum_{\alpha=2}^{\infty} y_\alpha \left[ (\eta_2-\eta_3)\eta_1^\alpha - (\eta_1-\eta_3)\eta_2^\alpha + (\eta_1-\eta_2)\eta_3^\alpha \right]. \end{aligned} \tag{C206}$$

Now consider the following combination:

$$\begin{aligned} f_1(1-\eta_3) - f_3(1-\eta_1) &= \sum_{\alpha=0}^{\infty} y_\alpha \left[ \eta_1^\alpha(1-\eta_3) - \eta_3^\alpha(1-\eta_1) \right] \\ &= (y_0+y_1)(\eta_1-\eta_3) + \sum_{\alpha=2}^{\infty} y_\alpha \left[ \eta_1^\alpha(1-\eta_3) - \eta_3^\alpha(1-\eta_1) \right] \\ &= (\eta_1-\eta_3)\left( 1 - \sum_{\alpha=2}^{\infty} y_\alpha \right) + \sum_{\alpha=2}^{\infty} y_\alpha \left[ \eta_1^\alpha(1-\eta_3) - \eta_3^\alpha(1-\eta_1) \right]. \end{aligned} \tag{C207}$$

From this we deduce

$$f_1(1-\eta_3) - f_3(1-\eta_1) - (\eta_1-\eta_3) = \sum_{\alpha=2}^{\infty} y_\alpha \left[ \eta_1^\alpha(1-\eta_3) - \eta_3^\alpha(1-\eta_1) - (\eta_1-\eta_3) \right]. \tag{C208}$$

We can now combine the two equalities (C206) and (C208) by subtracting the latter from the former. We obtain

$$\begin{aligned} &(\eta_2-\eta_3)f_1 - (\eta_1-\eta_3)f_2 + (\eta_1-\eta_2)f_3 - [f_1(1-\eta_3) - f_3(1-\eta_1) - (\eta_1-\eta_3)] \\ &= \sum_{\alpha=2}^{\infty} y_\alpha \left[ (\eta_2-1)\eta_1^\alpha - (\eta_1-\eta_3)\eta_2^\alpha + (1-\eta_2)\eta_3^\alpha + \eta_1 - \eta_3 \right] \\ &= \sum_{\alpha=2}^{\infty} y_\alpha \left[ (\eta_1-\eta_3)(1-\eta_2^\alpha) - (1-\eta_2)(\eta_1^\alpha - \eta_3^\alpha) \right]. \end{aligned} \tag{C209}$$

We now study the factors of the variables $y_\alpha$ in the last expression. For brevity, we label them as

$$g(\alpha) := (\eta_1-\eta_3)(1-\eta_2^\alpha) - (1-\eta_2)(\eta_1^\alpha - \eta_3^\alpha) \tag{C210}$$

and view $g(\alpha)$ as a continuous function of $\alpha \geq 2$. First, we observe that $g(\alpha)$ is always non-negative:

$$\begin{aligned} & g(\alpha) \geq 0 \\ \Leftrightarrow \quad & (\eta_1 - \eta_3)(1 - \eta_2^\alpha) \geq (1 - \eta_2)(\eta_1^\alpha - \eta_3^\alpha) \\ \Leftrightarrow \quad & (\eta_1 - \eta_3)(1 - \eta_2)(1 + \eta_2 + \cdots + \eta_2^{\alpha-1}) \\ & \geq (1 - \eta_2)(\eta_1 - \eta_3)(\eta_1^{\alpha-1} + \eta_1^{\alpha-2}\eta_3 + \cdots + \eta_1\eta_3^{\alpha-2} + \eta_3^{\alpha-1}), \end{aligned} \tag{C211}$$

which is verified since $1 \geq \eta_1$ and $\eta_2 \geq \eta_3$. Then, we notice that $g(\alpha)$ is a nondecreasing function of $\alpha$. Indeed, this amounts to showing that

$$\begin{aligned} & g(\alpha + 1) \geq g(\alpha) \\ \Leftrightarrow \quad & (\eta_1 - \eta_3)(1 - \eta_2^{\alpha+1}) - (1 - \eta_2)(\eta_1^{\alpha+1} - \eta_3^{\alpha+1}) \geq (\eta_1 - \eta_3)(1 - \eta_2^\alpha) - (1 - \eta_2)(\eta_1^\alpha - \eta_3^\alpha) \\ \Leftrightarrow \quad & (\eta_1 - \eta_3)(1 - \eta_2)\eta_2^\alpha + (1 - \eta_2)(1 - \eta_1)\eta_1^\alpha - (1 - \eta_2)(1 - \eta_3)\eta_3^\alpha \geq 0 \\ \Leftrightarrow \quad & (\eta_1 - \eta_3)\eta_2^\alpha + (1 - \eta_1)\eta_1^\alpha - (1 - \eta_3)\eta_3^\alpha \geq 0, \end{aligned} \tag{C212}$$

and a sufficient condition to prove the last inequality is obtained by one replacing $\eta_1^\alpha$ with $\eta_2^\alpha$ in the second term (since $\eta_1 > \eta_2$):

$$\begin{aligned} & (\eta_1 - \eta_3)\eta_2^\alpha + (1 - \eta_1)\eta_2^\alpha - (1 - \eta_3)\eta_3^\alpha \geq 0 \\ \Leftrightarrow \quad & (1 - \eta_3)\eta_2^\alpha - (1 - \eta_3)\eta_3^\alpha \geq 0, \end{aligned} \tag{C213}$$

where the last inequality is true since $\eta_2 > \eta_3$. Hence, we showed that $g(\alpha)$ is a nondecreasing function of $\alpha$ and, in particular, it holds that

$$g(\alpha) \geq g(2) \text{ for all } \alpha \geq 2. \tag{C214}$$

We now use the last expression in Eq. (C209) and derive the inequality

$$\begin{aligned} & (\eta_2 - \eta_3)f_1 - (\eta_1 - \eta_3)f_2 + (\eta_1 - \eta_2)f_3 - [f_1(1 - \eta_3) - f_3(1 - \eta_1) - (\eta_1 - \eta_3)] \\ & \geq g(2)\sum_{\alpha=2}^{\infty} y_\alpha \\ & = (\eta_1 - \eta_3)(1 - \eta_2)(1 + \eta_2 - \eta_1 - \eta_3)\sum_{\alpha=2}^{\infty} y_\alpha, \end{aligned} \tag{C215}$$

which leads to the following upper bound on the weight of the state $\bar{\sigma}$ outside the $(\leq 1)$-subspace:

$$\begin{aligned} \sum_{\alpha=2}^{\infty} y_\alpha &\leq \frac{(\eta_2 - \eta_3)f_1 - (\eta_1 - \eta_3)f_2 + (\eta_1 - \eta_2)f_3 - [f_1(1 - \eta_3) - f_3(1 - \eta_1) - (\eta_1 - \eta_3)]}{(\eta_1 - \eta_3)(1 - \eta_2)(1 + \eta_2 - \eta_1 - \eta_3)} \\ &= \frac{(1 - \eta_2)(f_3 - f_1) + (\eta_1 - \eta_3)(1 - f_2)}{(\eta_1 - \eta_3)(1 - \eta_2)(1 + \eta_2 - \eta_1 - \eta_3)}. \end{aligned} \tag{C216}$$

Then the upper bound in the original variables reads

$$\sum_{\alpha=2}^{\infty} \mathrm{Tr}\left[\bar{\sigma}\,\Pi_{\mathcal{Z}}^{\alpha}\right] \leq \overline{w}_{\mathcal{Z}}^{>1}, \tag{C217}$$

with

$$\overline{w}_{\mathcal{Z}}^{>1} := \min\left\{1, \frac{\overline{(\eta_\uparrow - \eta_\downarrow)Y^Z_{1,(\eta_2,\eta_2)} - (1 - \eta_2)(Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)} - Y^Z_{1,(\eta_\uparrow,\eta_\uparrow)}) - (\eta_\uparrow - \eta_\downarrow)p_d^{\mathcal{Z}}}}{(1 - p_d^{\mathcal{Z}})(\eta_\uparrow - \eta_\downarrow)(1 - \eta_2)(1 + \eta_2 - \eta_\uparrow - \eta_\downarrow)}\right\}, \tag{C218}$$

where in Appendix D we derive an upper bound tailored to the specific combination of yields in the numerator.

The bound in Eq. (C217) plays a crucial role in reducing the calculation of the phase error rate to the subspace with at most one photon in $\mathcal{Z}$, as we show in the next part of the proof.

### *e. Reduction of the phase error rate to the (≤1)-subspace*

We now use Eq. (C180), derived for the detection POVM element $Z_{\checkmark}$, in the numerator of the phase error rate (C94). By combining this with the upper bound in Eq. (C217), we reduce the calculation of the phase error rate to the subspace defined by $\Pi^0_{\mathcal{Z}} + \Pi^1_{\mathcal{Z}}$.

To start with, from Eq. (C180) we compute

$$\sqrt{Z_{\checkmark}} = M^{\leq 1}_{\mathcal{Z}} + M^{>1}_{\mathcal{Z}}, \tag{C219}$$

where we introduced two positive-semidefinite operators

$$M^{\leq 1}_{\mathcal{Z}} = \sum_{\alpha=0}^{1} \sqrt{p_{\checkmark|\alpha}}\,\Pi^{\alpha}_{\mathcal{Z}}, \tag{C220}$$

$$M^{>1}_{\mathcal{Z}} = \sum_{\alpha=2}^{\infty} \sqrt{p_{\checkmark|\alpha}}\,\Pi^{\alpha}_{\mathcal{Z}}. \tag{C221}$$

With the use of Eq. (C219), the numerator of the phase error rate in Eq. (C94) decomposes into three contributions:

$$\tilde{e}_{X,1} Y^{Z}_{1,(\eta_\downarrow,\eta_\downarrow)} = \frac{1}{d}\sum_{k=0}^{d-1} \mathrm{Tr}\left[\sigma_k \sqrt{Z_{\checkmark}} \sum_{k'\neq k} \tilde{X}_{k'} \sqrt{Z_{\checkmark}}\right] = \Delta_1 + \Delta_2 + \Delta_3, \tag{C222}$$

where

$$\Delta_1 = \frac{1}{d}\sum_{k=0}^{d-1} \mathrm{Tr}\left[\sigma_k M^{\leq 1}_{\mathcal{Z}} \sum_{k'\neq k} \tilde{X}_{k'} M^{\leq 1}_{\mathcal{Z}}\right], \tag{C223}$$

$$\Delta_2 = \frac{1}{d}\sum_{k=0}^{d-1} \mathrm{Tr}\left[\sigma_k (M^{\leq 1}_{\mathcal{Z}} \sum_{k'\neq k} \tilde{X}_{k'} M^{>1}_{\mathcal{Z}} + \mathrm{H.c.})\right], \tag{C224}$$

$$\Delta_3 = \frac{1}{d}\sum_{k=0}^{d-1} \mathrm{Tr}\left[\sigma_k M^{>1}_{\mathcal{Z}} \sum_{k'\neq k} \tilde{X}_{k'} M^{>1}_{\mathcal{Z}}\right], \tag{C225}$$

where "H.c." stands for the Hermitian conjugate of the term in parentheses.

While for the term $\Delta_1$ the only components of the states $\sigma_k$ that contribute are those localized in the ($\leq 1$)-subspace (due to $M^{\leq 1}_{\mathcal{Z}}$), the other two terms ($\Delta_2$ and $\Delta_3$) receive contributions from infinitely many subspaces with an arbitrary number of photons in the interval $\mathcal{Z}$. As we show later, the statistics collected for different TBS settings allow us to estimate the contributions to the phase error rate coming from states in the ($\leq 1$)-subspace. Hence, we can precisely estimate the value of $\Delta_1$. Conversely, we upper-bound $\Delta_2$ and $\Delta_3$ by virtue of our characterization of the weight of the states $\sigma_k$ in the subspace with more than one photon in $\mathcal{Z}$, embodied by the upper bound (C217).

We start by deriving an upper bound on $\Delta_3$. The fact that $\mathbb{1} - \sum_{k'\neq k}\tilde{X}_{k'} \geq 0$ holds implies that $M^{>1}_{\mathcal{Z}}(\mathbb{1} - \sum_{k'\neq k}\tilde{X}_{k'})M^{>1}_{\mathcal{Z}} \geq 0$ also holds and thus that

$$\begin{aligned} M^{>1}_{\mathcal{Z}} \sum_{k'\neq k}\tilde{X}_{k'} M^{>1}_{\mathcal{Z}} &\leq (M^{>1}_{\mathcal{Z}})^2 \\ &= \sum_{\alpha=2}^{\infty} p_{\checkmark|\alpha}\,\Pi^{\alpha}_{\mathcal{Z}} \\ &\leq \sum_{\alpha=2}^{\infty} \Pi^{\alpha}_{\mathcal{Z}}, \end{aligned} \tag{C226}$$

where we used the fact that $\Pi^{\alpha}_{\mathcal{Z}}$ are orthogonal projectors and that $p_{\checkmark|\alpha}$ are probabilities. Then Eq. (C226) implies the following bound on $\Delta_3$:

$$\begin{aligned}\Delta_3 &\leq \sum_{\alpha=2}^{\infty} \mathrm{Tr}\left[\bar{\sigma}\,\Pi^{\alpha}_{\mathcal{Z}}\right] \\ &\leq \overline{w}^{\geq 1}_{\mathcal{Z}},\end{aligned} \tag{C227}$$

where we used Eqs. (C173) and (C217).

We now derive an upper bound on the term $\Delta_2$ in Eq. (C222), taking inspiration from Appendix B in Ref. [57]. First, we recast $\Delta_2$ as follows:

$$\Delta_2 = \frac{1}{d}\textstyle\sum_{k=0}^{d-1} \mathrm{Tr}[H_k \Gamma_k], \tag{C228}$$

where for brevity we introduced the positive operator $\Gamma_k$ and the self-adjoint operator $H_k$,

$$H_k := M^{\leq 1}_{\mathcal{Z}} \sigma_k M^{\geq 1}_{\mathcal{Z}} + \mathrm{H.c.}, \tag{C229}$$

$$\Gamma_k := \textstyle\sum_{k' \neq k} \tilde{X}_{k'}. \tag{C230}$$

Since $H_k$ is self-adjoint, we can decompose it as

$$H_k = H_k^{+} - H_k^{-} \tag{C231}$$

for some positive operators $H_k^{+}$ and $H_k^{-}$. Then we can upper-bound $\Delta_2$ by

$$\begin{aligned}\Delta_2 &= \frac{1}{d}\textstyle\sum_{k=0}^{d-1} \left(\mathrm{Tr}[H_k^{+}\Gamma_k] - \mathrm{Tr}[H_k^{-}\Gamma_k]\right) \\ &\leq \frac{1}{d}\textstyle\sum_{k=0}^{d-1} \mathrm{Tr}[H_k^{+}\Gamma_k] \\ &\leq \frac{1}{d}\textstyle\sum_{k=0}^{d-1} \mathrm{Tr}[H_k^{+}],\end{aligned} \tag{C232}$$

where in the first inequality we used the fact that the trace of the product of two positive operators is non-negative, and in the second inequality that $\Gamma_k \leq \mathbb{1}$. Now we use Eq. (C173) to define the self-adjoint operator

$$H := M^{\leq 1}_{\mathcal{Z}} \bar{\sigma} M^{\geq 1}_{\mathcal{Z}} + \mathrm{H.c.} \tag{C233}$$

and observe that $H$, through Eqs. (C229) and (C231), can be written as the difference of two positive operators:

$$\begin{aligned}H &= \frac{1}{d}\textstyle\sum_{k=0}^{d-1} H_k^{+} - \frac{1}{d}\sum_{k=0}^{d-1} H_k^{-} &\text{(C234)}\\ &\equiv H^{+} - H^{-}. &\text{(C235)}\end{aligned}$$

Hence, by definition of the one-norm, it holds that

$$\|H\|_1 = \mathrm{Tr}[H^{+}] + \mathrm{Tr}[H^{-}]. \tag{C236}$$

Moreover, since $\mathrm{Tr}[H] = 0$ by the definition of $H$, we have

$$\mathrm{Tr}[H^{+}] = \mathrm{Tr}[H^{-}] = \frac{1}{2}\|H\|_1 . \tag{C237}$$

By using this in Eq. (C232), we obtain

$$\Delta_2 \leq \frac{1}{2}\|H\|_1 . \tag{C238}$$

Now we use the definition of $H$ in Eq. (C233) to compute

$$\begin{aligned}\Delta_2 &\leq \frac{1}{2}\mathrm{Tr}[\sqrt{H^2}] \\ &= \frac{1}{2}\mathrm{Tr}\left[\sqrt{M^{\leq 1}_{\mathcal{Z}}\bar{\sigma}\left(M^{\geq 1}_{\mathcal{Z}}\right)^2 \bar{\sigma} M^{\leq 1}_{\mathcal{Z}}}\right] \\ &\quad + \frac{1}{2}\mathrm{Tr}\left[\sqrt{M^{\geq 1}_{\mathcal{Z}}\bar{\sigma}\left(M^{\leq 1}_{\mathcal{Z}}\right)^2 \bar{\sigma} M^{\geq 1}_{\mathcal{Z}}}\right] \\ &= \left\| M^{\leq 1}_{\mathcal{Z}}\bar{\sigma} M^{\geq 1}_{\mathcal{Z}}\right\|_1 ,\end{aligned} \tag{C239}$$

where we used the fact that $M^{\leq 1}_{\mathcal{Z}}$ and $M^{\geq 1}_{\mathcal{Z}}$ have orthogonal support and that $\|A\|_1 = \mathrm{Tr}[\sqrt{A^{\dagger}A}] = \mathrm{Tr}[\sqrt{AA^{\dagger}}]$. From Eq. (3) in Ref. [58], which we report here for clarity,

$$\left\|A^{\dagger}B\right\|_1 \leq \sqrt{\mathrm{Tr}[AA^{\dagger}]\,\mathrm{Tr}[BB^{\dagger}]}, \tag{C240}$$

we can upper-bound the right-hand side of Eq. (C239) with the choices $A^{\dagger} = M^{\leq 1}_{\mathcal{Z}}\sqrt{\bar{\sigma}}$ and $B = \sqrt{\bar{\sigma}} M^{\geq 1}_{\mathcal{Z}}$ as follows:

$$\begin{aligned}\Delta_2 &\leq \sqrt{\mathrm{Tr}\left[\bar{\sigma}\left(M^{\leq 1}_{\mathcal{Z}}\right)^2\right]\mathrm{Tr}\left[\bar{\sigma}\left(M^{\geq 1}_{\mathcal{Z}}\right)^2\right]} \\ &= \sqrt{\left\{\mathrm{Tr}\left[\bar{\sigma}Z_{\checkmark}\right] - \mathrm{Tr}\left[\bar{\sigma}\left(M^{\geq 1}_{\mathcal{Z}}\right)^2\right]\right\}\mathrm{Tr}\left[\bar{\sigma}\left(M^{\geq 1}_{\mathcal{Z}}\right)^2\right]},\end{aligned} \tag{C241}$$

where in the last equality we used Eq. (C219). Now we notice that $\mathrm{Tr}\left[\bar{\sigma}Z_{\checkmark}\right] = Y^{Z}_{1,(\eta_{\downarrow},\eta_{\downarrow})}$ by Eq. (C172). Moreover, from the derivation of the bound on $\Delta_3$ we know that

$$0 \leq \mathrm{Tr}\left[\bar{\sigma}\left(M^{\geq 1}_{\mathcal{Z}}\right)^2\right] \leq \overline{w}^{\geq 1}_{\mathcal{Z}}. \tag{C242}$$

Thus, we can upper-bound the right-hand side of Eq. (C241) as follows:

$$\Delta_2 \leq \max_{x\in[0,\overline{w}^{\geq 1}_{\mathcal{Z}}]} \sqrt{\left(\overline{Y^{Z}_{1,(\eta_{\downarrow},\eta_{\downarrow})}} - x\right)x}, \tag{C243}$$

where we replaced the yield with an upper bound derived with the decoy-state method (see Appendix D). Finally, we solve the optimization in the last expression and obtain

$$\Delta_2 \leq \sqrt{\left(\overline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}} - \min\left\{\overline{w}^{>1}_{\mathcal{Z}}, \frac{\overline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}}{2}\right\}\right)\min\left\{\overline{w}^{>1}_{\mathcal{Z}}, \frac{\overline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}}{2}\right\}}. \tag{C244}$$

In a similar way, one could derive a lower bound on $\Delta_2$. In particular, one can lower-bound $\Delta_2$ starting from Eq. (C232),

$$\begin{aligned}\Delta_2 &= \frac{1}{d}\textstyle\sum_{k=0}^{d-1}\left(\mathrm{Tr}[H_k^+\Gamma_k] - \mathrm{Tr}[H_k^-\Gamma_k]\right)\\ &\geq -\frac{1}{d}\textstyle\sum_{k=0}^{d-1}\mathrm{Tr}[H_k^-\Gamma_k]\\ &\geq -\frac{1}{d}\textstyle\sum_{k=0}^{d-1}\mathrm{Tr}[H_k^-]\\ &= -\mathrm{Tr}[H^-],\end{aligned} \tag{C245}$$

and then use the result in Eq. (C237) to upper-bound $\mathrm{Tr}[H^-]$, thus obtaining

$$\Delta_2 \geq -\sqrt{\left(\overline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}} - \min\left\{\overline{w}^{>1}_{\mathcal{Z}}, \frac{\overline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}}{2}\right\}\right)\min\left\{\overline{w}^{>1}_{\mathcal{Z}}, \frac{\overline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}}{2}\right\}}. \tag{C246}$$

By using Eqs. (C227) and (C244) in Eq. (C222), we arrive at the following upper bound on the numerator of the phase error rate:

$$\tilde{e}_{X,1}Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)} \leq \Delta_1 + \overline{\Delta_2} + \overline{w}^{>1}_{\mathcal{Z}}, \tag{C247}$$

where $\overline{w}^{>1}_{\mathcal{Z}}$ is given in Eq. (C218), while $\overline{\Delta_2}$ and $\Delta_1$ are defined as

$$\overline{\Delta_2} = \sqrt{\left(\overline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}} - \min\left\{\overline{w}^{>1}_{\mathcal{Z}}, \frac{\overline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}}{2}\right\}\right)\min\left\{\overline{w}^{>1}_{\mathcal{Z}}, \frac{\overline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}}{2}\right\}}, \tag{C248}$$

$$\Delta_1 = \frac{1}{d}\textstyle\sum_{k=0}^{d-1}\mathrm{Tr}\left[\sigma_k M^{\leq 1}_{\mathcal{Z}}\sum_{k'\neq k}\tilde{X}_{k'}M^{\leq 1}_{\mathcal{Z}}\right], \tag{C249}$$

and $M^{\leq 1}_{\mathcal{Z}}$ is given in Eq. (C220).

As anticipated, the right-hand side of the bound in Eq. (C247) depends (through $\Delta_1$) only on the statistics generated by states that contain up to one photon in the interval $\mathcal{Z}$. In particular, $\Delta_1$ is linked to the error rate in distinguishing the $X$-basis states sent by Alice with Bob's test measurement, Eq. (C15), and can be estimated with the rich statistics of the test rounds. For this, we now focus on deriving explicit expressions for Bob's POVM elements, Eq. (C6).

### *f. Bob's X-basis detector*

The detection statistics that are needed to estimate $\Delta_1$ are those generated by the following reduced POVM elements:

$$X^{(\eta_i,\eta_l)}_{k,\checkmark} := \sum_{j=0}^{d-1} M^{(\eta_i,\eta_l)}_{j,k}, \tag{C250}$$

$$X^{(\eta_i,\eta_l)}_{k,\emptyset} := M^{(\eta_i,\eta_l)}_{\emptyset,k}, \tag{C251}$$

where we ignore the specific outcome of the $Z$-basis detector and register onnly whether it clicks or does not click. Note that Bob's test measurement, as defined in Eq. (C15), is recovered from Eqs. (C250) and (C251) as follows:

$$X_k = X_{k,\checkmark}^{(\eta_\uparrow,\eta_\uparrow)} + X_{k,\emptyset}^{(\eta_\uparrow,\eta_\uparrow)}. \tag{C252}$$

Our goal is to derive explicit expressions for the POVM elements (acting on mode $a$) given in Eqs. (C250) and (C251).

The first step is to describe the ideal $X$-basis detector acting on mode $e$ in Fig. 7. Let $D := \{0, 1, \ldots, d-1\}$ be the set of outcomes of the $X$-basis detector on mode $e$ and let $\mathcal{P}(D)$ be the power set of $D$. Recall that we assumed that Bob maps multiclick events $K \in \mathcal{P}(D)$, i.e., events with clicks in the physical modes $\mathcal{X}_l$, for $l \in K$, to a single outcome. This can be formalized by an un-normalized right stochastic matrix $P \in \mathrm{M}_{\mathcal{P}(D)\setminus\emptyset \times d}$, with elements

$$\{P\}_{K,k} := \Pr(k|K)\ , \tag{C253}$$

where $\Pr(k|K)$ represents the probability that the multiclick event $K$ is mapped to the single outcome $k$. As explained in Sec. III, we assume that the following holds:

$$\sum_{k=0}^{d-1} \Pr(k|K) = 1 \quad \text{for all } K \in \mathcal{P}(D) \setminus \emptyset, \tag{C254}$$

i.e., that no event with at least one click is assigned to the no-detection event. In other words, every time there is at least one click (event $K \neq \emptyset$), Bob assigns the event to outcome $k$ according to the distribution $\Pr(k|K)$. Then, the POVM element corresponding to a detection of outcome $k$, in the absence of dark counts, is given by

$$(X_k)_e = \sum_{K\in\mathcal{P}(D)\setminus\emptyset} \Pr(k|K)\ \Pi_K^{\geq 1}, \tag{C255}$$

where $\Pi_K^{\geq 1}$ is the projector on the subspace with at least one photon in mode $\mathcal{X}_l$ for each $l \in K$, and no photons in the other measured modes $\mathcal{X}_m$ for $m \notin K$. Note that the event $K = \emptyset$ is excluded from Eq. (C255) since no-detection events are not mapped to measurement outcomes. We now consider that each mode $\mathcal{X}_k$ may click with probability $p_d^X$, given that no photon is in that mode. Thus, we deduce that even the events where some of the clicks are caused by dark counts are mapped according to Eq. (C253), since Bob has no way to distinguish dark counts from actual detections. Therefore, the POVM element for outcome $k$ in the presence of dark counts becomes

$$(X_k)_e = \sum_{K\in\mathcal{P}(D)\setminus\emptyset} \Pr(k|K)\ X_K, \tag{C256}$$

where $X_K$ is the POVM element corresponding to the multiclick event $K$. Clearly, $X_K$ receives contributions from $\Pi_K^{\geq 1}$, but also from all the projectors $\Pi_S^{\geq 1}$, where $S \in \mathcal{P}(K)$ can be interpreted as the set of "genuine" clicks (i.e., clicks caused by photons) in the multiclick event $K$, provided that $|K| - |S|$ dark counts also occur ($|K|$ represents the number of elements in $K$). In conclusion, we have

$$X_K = \sum_{S\in\mathcal{P}(K)} (p_d^X)^{|K|-|S|}(1-p_d^X)^{d-|K|}\ \Pi_S^{\geq 1}. \tag{C257}$$

*Remark 5.* By using Eqs. (C256) and (C257) in the computation of the POVM element corresponding to a detection in any outcome, $(X_\checkmark)_e$, one obtains

$$(X_\checkmark)_e = \sum_{k=0}^{d-1} (X_k)_e \tag{C258}$$

$$= \left[1-(1-p_d^X)^d\right]\Pi_\emptyset^{\geq 1} + \sum_{X\in\mathcal{P}(D)\setminus\emptyset} \Pi_X^{\geq 1}, \tag{C259}$$

which coincides with the analogous POVM element in the $Z$ basis, Eq. (C155), by using Eq. (B3) and by identifying $\Pi_\emptyset^{\geq 1} = \Pi_{\mathcal{X}}^0$ and $\sum_{X\in\mathcal{P}(D)\setminus\emptyset} \Pi_X^{\geq 1} = \sum_{\beta=1}^\infty \Pi_{\mathcal{X}}^\beta$, with $\Pi_{\mathcal{X}}^\beta$ being the analogue for the $X$ basis of $\Pi_{\mathcal{Z}}^\alpha$ for the $Z$ basis, namely, the projector on the subspace with $\beta$ photons in the interval $\mathcal{X}$ and any number of photons outside $\mathcal{X}$. With these substitutions, we obtain

$$(X_\checkmark)_e = p_d^{\mathcal{X}}\mathbb{1} + (1-p_d^{\mathcal{X}})\sum_{\beta=1}^\infty \Pi_{\mathcal{X}}^\beta. \tag{C260}$$

Now we can compute the POVM element corresponding to outcome $k$ in the $X$-basis detector, acting on the transmitted mode $c$. According to the model in Fig. 7 and by one following the same approach that led to the derivation of Eq. (C175) this will be given by

$$(X_k)_c = \langle \mathrm{vac}|_d\, U^\dagger(\eta_r)(X_k)_e \otimes \mathbb{1}_f\, U(\eta_r)\, |\mathrm{vac}\rangle_d\,. \tag{C261}$$

Alternatively, a faster way to obtain $(X_k)_c$ is to observe that when each photon can be lost independently with probability $1-\eta_r$, the POVM element $X_K$ of the multiclick event $K$ receives contributions from any possible configuration of photons arriving at the detector. Thus, the relevant projector to express the operator in Eq. (C261) becomes

$$\Pi_{\mathcal{X}}^{\alpha_0,\alpha_1,\ldots,\alpha_{d-1}}, \tag{C262}$$

which is defined as the projector on the subspace with $\alpha_k$ photons in mode $\mathcal{X}_k$, for $k = 0, \ldots, d-1$. Moreover, we note that $X_K$ will have the same structure as in Eq. (C257) if we interpret $S$ as the set of modes that contain at least one

photon after considering the detector's nonunit efficiency [i.e., after applying $U(\eta_r)$]:

$$X_K = \sum_{S\in\mathcal{P}(K)} (p_d^X)^{|K|-|S|}(1-p_d^X)^{d-|K|}\, M_S^{\geq 1}, \tag{C263}$$

where $M_S^{\geq 1}$ is the POVM element of at least one photon in mode $\mathcal{X}_s$, after loss, for every $s \in S$. Thus, we can easily express $M_S^{\geq 1}$ in terms of the projectors (C262) as follows:

$$M_S^{\geq 1} = \sum_{\alpha_0,\alpha_1,\ldots,\alpha_{d-1}=0}^{\infty} \Pi_{\mathcal{X}}^{\alpha_0,\alpha_1,\ldots,\alpha_{d-1}} \prod_{s\in S}[1-(1-\eta_r)^{\alpha_s}] \times \prod_{r\in S^c}(1-\eta_r)^{\alpha_r}, \tag{C264}$$

where $S^c = D \setminus S$ is the complement of $S$ in $D$.

In conclusion, the POVM element for outcome $k$ in the $X$-basis detector with efficiency $\eta_r$ and dark count probability $p_d^X$ per mode is given by

$$(X_k)_c = \sum_{K\in\mathcal{P}(D)\setminus\emptyset} \Pr(k|K) \times \sum_{S\in\mathcal{P}(K)} (p_d^X)^{|K|-|S|}(1-p_d^X)^{d-|K|}\, M_S^{\geq 1}, \tag{C265}$$

with $M_S^{\geq 1}$ given in Eq. (C264). Moreover, it will turn out to be useful to calculate the POVM element corresponding to a detection of any outcome in mode $c$. This is achieved from Eq. (C261) as follows:

$$\begin{aligned}(X_\checkmark)_c &= \sum_{k=0}^{d-1}(X_k)_c \\ &= \langle \mathrm{vac}|_d\, U^\dagger(\eta_r)(X_\checkmark)_e \otimes \mathbb{1}_f\, U(\eta_r)\,|\mathrm{vac}\rangle_d \\ &= p_d^{\mathcal{X}}\mathbb{1}_c + (1-p_d^{\mathcal{X}})\,\langle \mathrm{vac}|_d\, U^\dagger(\eta_r) \\ &\quad\times \sum_{\beta=1}^{\infty}(\Pi_{\mathcal{X}}^{\beta})_e \otimes \mathbb{1}_f\, U(\eta_r)\,|\mathrm{vac}\rangle_d,\end{aligned} \tag{C266}$$

where we used Eq. (C260) from Remark 5 in the last equality. Now we use the fact that a calculation similar to the one above has already been done for computing Eq. (C176) and resulted in Eq. (C178). Analogously, we obtain

$$\begin{aligned}(X_\checkmark)_c &= p_d^{\mathcal{X}}\mathbb{1}_c + (1-p_d^{\mathcal{X}})\sum_{\beta=1}^{\infty}\left[1-(1-\eta_r)^{\beta}\right](\Pi_{\mathcal{X}}^{\beta})_c \\ &= \sum_{\beta=0}^{\infty}\left[1-(1-p_d^{\mathcal{X}})(1-\eta_r)^{\beta}\right](\Pi_{\mathcal{X}}^{\beta})_c.\end{aligned} \tag{C267}$$

Now we have all the ingredients to compute the POVM elements defined in Eqs. (C250) and (C251). According to the scheme in Fig. 7, we have

$$X_{k,\checkmark}^{(\eta_i,\eta_l)} = \langle \mathrm{vac}|_b\, U_{(\eta_i,\eta_l)}^\dagger (X_k)_c \otimes (Z_\checkmark)_{c'} U_{(\eta_i,\eta_l)}\,|\mathrm{vac}\rangle_b\,, \tag{C268}$$

$$X_{k,\emptyset}^{(\eta_i,\eta_l)} = \langle \mathrm{vac}|_b\, U_{(\eta_i,\eta_l)}^\dagger (X_k)_c \otimes (Z_\emptyset)_{c'} U_{(\eta_i,\eta_l)}\,|\mathrm{vac}\rangle_b\,, \tag{C269}$$

where $(X_k)_c$ is given in Eq. (C265), $(Z_\checkmark)_{c'}$ is given in Eq. (C155), and $(Z_\emptyset)_{c'} = \mathbb{1}_{c'} - (Z_\checkmark)_{c'}$.

Now that we have derived the POVM elements of interest, in the following subsection we link them to the corresponding one-photon yields and bit error rates, which in turn will be used to bound $\Delta_1$ in Eq. (C247).

### *g. One-photon X-basis yields and bit error rates*

By applying the decoy-state method on the detection statistics of the test rounds (see Appendix D), Alice and Bob can estimate the following one-photon $X$-basis yields, which we call the "test-round yields":

$$Y_{1,(\eta_i,\eta_l)}^{X,\checkmark} = \textstyle\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}X_{\checkmark,\checkmark}^{(\eta_i,\eta_l)}\right], \tag{C270}$$

$$Y_{1,(\eta_i,\eta_l)}^{X,\emptyset} = \textstyle\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}X_{\checkmark,\emptyset}^{(\eta_i,\eta_l)}\right], \tag{C271}$$

where we defined

$$X_{\checkmark,\checkmark}^{(\eta_i,\eta_l)} = \sum_{k=0}^{d-1} X_{k,\checkmark}^{(\eta_i,\eta_l)}, \tag{C272}$$

$$X_{\checkmark,\emptyset}^{(\eta_i,\eta_l)} = \sum_{k=0}^{d-1} X_{k,\emptyset}^{(\eta_i,\eta_l)}. \tag{C273}$$

Similarly, by applying the decoy-state method on the $X$-basis gains (12) and (13) and on the $X$-basis QBERs (15) and (16), the parties can estimate the following one-photon $X$-basis bit error rates, also called the "test-round bit error rates":

$$e_{X,1,(\eta_i,\eta_l),\checkmark} = \frac{\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}\sum_{k'\neq k}X_{k',\checkmark}^{(\eta_i,\eta_l)}\right]}{Y_{1,(\eta_i,\eta_l)}^{X,\checkmark}}, \tag{C274}$$

$$e_{X,1,(\eta_i,\eta_l),\emptyset} = \frac{\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}\sum_{k'\neq k}X_{k',\emptyset}^{(\eta_i,\eta_l)}\right]}{Y_{1,(\eta_i,\eta_l)}^{X,\emptyset}}. \tag{C275}$$

We observe that the test-round yields, Eqs. (C270) and (C271), and the test-round bit error rates, Eqs. (C274) and (C275), do not depend only on the component of $\sigma_k$ in the $(\leq 1)$-subspace.

Conversely, this is the only component that matters when one is computing $\Delta_1$ [see Eq. (C249)]. Therefore, similarly to the derivation of the upper bound on the phase error rate (C247), we now derive upper and lower bounds on the test-round yields and test-round bit error rates such that they depend only on the ($\leq 1$)-subspace component of $\sigma_k$. The derivation of the bounds is identical for each of the four equations— Eqs. (C270), (C271), (C274), and (C275); thus, we focus on deriving the bounds for Eq. (C274). The first step entails our using the fact that $\sum_{\alpha=0}^{\infty}\Pi_{\mathcal{Z}}^{\alpha}=\mathbb{1}$, such that the numerator in (C274) can be recast as follows:

$$\begin{aligned} Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}e_{X,1,(\eta_i,\eta_l),\checkmark} &= \sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}\left(\sum_{\alpha=0}^{\infty}\Pi_{\mathcal{Z}}^{\alpha}\right)\sum_{k'\neq k}X^{(\eta_i,\eta_l)}_{k',\checkmark}\left(\sum_{\alpha=0}^{\infty}\Pi_{\mathcal{Z}}^{\alpha}\right)\right] \\ &= \sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}\Pi_{\mathcal{Z}}^{\leq 1}\sum_{k'\neq k}X^{(\eta_i,\eta_l)}_{k',\checkmark}\Pi_{\mathcal{Z}}^{\leq 1}\right]+\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}\left(\Pi_{\mathcal{Z}}^{\leq 1}\sum_{k'\neq k}X^{(\eta_i,\eta_l)}_{k',\checkmark}\Pi_{\mathcal{Z}}^{>1}+\mathrm{H.c.}\right)\right] \\ &\quad+\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}\Pi_{\mathcal{Z}}^{>1}\sum_{k'\neq k}X^{(\eta_i,\eta_l)}_{k',\checkmark}\Pi_{\mathcal{Z}}^{>1}\right], \end{aligned} \tag{C276}$$

where we defined the projectors

$$\Pi_{\mathcal{Z}}^{\leq 1}:=\Pi_{\mathcal{Z}}^{0}+\Pi_{\mathcal{Z}}^{1}, \tag{C277}$$

$$\Pi_{\mathcal{Z}}^{>1}:=\sum_{\alpha=2}^{\infty}\Pi_{\mathcal{Z}}^{\alpha}. \tag{C278}$$

The three terms in Eq. (C276) closely resemble the three terms $\Delta_1$, $\Delta_2$, and $\Delta_3$ defined in Eq. (C222) for the phase error rate. One can easily verify that the second and third terms in Eq. (C276) can be bounded in an analogous manner to $\Delta_2$ and $\Delta_3$. In particular, for the third term we obtain

$$\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}\Pi_{\mathcal{Z}}^{>1}\sum_{k'\neq k}X^{(\eta_i,\eta_l)}_{k',\checkmark}\Pi_{\mathcal{Z}}^{>1}\right]\leq\overline{w}_{\mathcal{Z}}^{>1}, \tag{C279}$$

where we used Eq. (C227). For the second term we can follow the derivation of the bound on $\Delta_2$ until Eq. (C241), which in this case becomes

$$\begin{aligned} \sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}\left(\Pi_{\mathcal{Z}}^{\leq 1}\sum_{k'\neq k}X^{(\eta_i,\eta_l)}_{k',\checkmark}\Pi_{\mathcal{Z}}^{>1}+\mathrm{H.c.}\right)\right] &\leq\sqrt{\left\{1-\mathrm{Tr}\left[\bar{\sigma}\,\Pi_{\mathcal{Z}}^{>1}\right]\right\}\mathrm{Tr}\left[\bar{\sigma}\,\Pi_{\mathcal{Z}}^{>1}\right]} \\ &\leq\sqrt{\overline{w}_{\mathcal{Z}}^{>1}}. \end{aligned} \tag{C280}$$

By using Eqs. (C280) and (C279) in Eq. (C276), we obtain the following upper bound on the numerator of the test-round bit error rate:

$$Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}e_{X,1,(\eta_i,\eta_l),\checkmark}\leq\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}e_{X,1,(\eta_i,\eta_l),\checkmark}\right]_{\mathcal{Z}}^{\leq 1}+\sqrt{\overline{w}_{\mathcal{Z}}^{>1}}+\overline{w}_{\mathcal{Z}}^{>1}, \tag{C281}$$

where $\overline{w}_{\mathcal{Z}}^{>1}$ is given in Eq. (C218) and where we defined

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}e_{X,1,(\eta_i,\eta_l),\checkmark}\right]_{\mathcal{Z}}^{\leq 1}:=\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}\Pi_{\mathcal{Z}}^{\leq 1}\sum_{k'\neq k}X^{(\eta_i,\eta_l)}_{k',\checkmark}\Pi_{\mathcal{Z}}^{\leq 1}\right] \tag{C282}$$

as the numerator of the bit error rate when the state is restricted to the ($\leq 1$)-subspace. To derive a lower bound on the numerator of the test-round bit error rate, we use the fact that

$$\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}\Pi_{\mathcal{Z}}^{>1}\sum_{k'\neq k}X^{(\eta_i,\eta_l)}_{k',\checkmark}\Pi_{\mathcal{Z}}^{>1}\right]\geq 0, \tag{C283}$$

since $\Pi_{\mathcal{Z}}^{>1}\sum_{k'\neq k}X^{(\eta_i,\eta_l)}_{k',\checkmark}\Pi_{\mathcal{Z}}^{>1}\geq 0$. For the second term in Eq. (C276), we can obtain a lower bound in an way analogous to the derivation of the lower bound on $\Delta_2$ in Eq. (C246). We obtain

$$\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}\left(\Pi_{\mathcal{Z}}^{\leq 1}\sum_{k'\neq k}X^{(\eta_i,\eta_l)}_{k',\checkmark}\Pi_{\mathcal{Z}}^{>1}+\mathrm{H.c.}\right)\right]\geq-\sqrt{\overline{w}_{\mathcal{Z}}^{>1}}. \tag{C284}$$

By using Eqs. (C283) and (C284) in Eq. (C276), we obtain the following lower bound on the numerator of the test-round bit error rate:

$$Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark} \geq \left[ Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark} \right]^{\leq 1}_{\mathcal{Z}} - \sqrt{\overline{w}^{>1}_{\mathcal{Z}}}. \tag{C285}$$

Bounds similar to Eqs. (C281) and (C285) can be obtained for the other test-round bit error rate (C275) and for the test-round yields (C270) and (C271). Such bounds are important as they allow us to estimate the test-round yields and the (numerator of) the test-round bit error rates, when restricted to the ($\leq 1$)-subspace, with significant accuracy. Indeed, we can derive a narrow interval of existence for the quantity defined in Eq. (C282) by combining Eqs. (C281) and (C285):

$$\underline{\left[ Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark} \right]^{\leq 1}_{\mathcal{Z}}} \leq \left[ Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark} \right]^{\leq 1}_{\mathcal{Z}} \leq \overline{\left[ Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark} \right]^{\leq 1}_{\mathcal{Z}}}, \tag{C286}$$

where we defined

$$\underline{\left[ Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark} \right]^{\leq 1}_{\mathcal{Z}}} := \max \left\{ 0, \underline{Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}} - \sqrt{\overline{w}^{>1}_{\mathcal{Z}}} - \overline{w}^{>1}_{\mathcal{Z}} \right\}, \tag{C287}$$

$$\overline{\left[ Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark} \right]^{\leq 1}_{\mathcal{Z}}} := \min \left\{ 1, \overline{Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}} + \sqrt{\overline{w}^{>1}_{\mathcal{Z}}} \right\}, \tag{C288}$$

and used the fact that $0 \leq \Pi^{\leq 1}_{\mathcal{Z}} \sum_{k' \neq k} X^{(\eta_i,\eta_l)}_{k',\checkmark} \Pi^{\leq 1}_{\mathcal{Z}} \leq \mathbb{1}$. Note that we replaced the product of the test-round yield and bit error rate with the respective upper or lower bound obtained from the decoy-state method (derived in Appendix D), such that Eqs. (C287) and (C288) are exclusively given in terms of observed quantities.

Analogously, we define the restriction of the test-round bit error rate in Eq. (C275) to the ($\leq 1$)-subspace as

$$\left[ Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset} \right]^{\leq 1}_{\mathcal{Z}} := \sum_{k=0}^{d-1} \mathrm{Tr} \left[ \frac{\sigma_k}{d} \Pi^{\leq 1}_{\mathcal{Z}} \sum_{k' \neq k} X^{(\eta_i,\eta_l)}_{k',\emptyset} \Pi^{\leq 1}_{\mathcal{Z}} \right], \tag{C289}$$

and derive the interval of existence:

$$\underline{\left[ Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset} \right]^{\leq 1}_{\mathcal{Z}}} \leq \left[ Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset} \right]^{\leq 1}_{\mathcal{Z}} \leq \overline{\left[ Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset} \right]^{\leq 1}_{\mathcal{Z}}}, \tag{C290}$$

with

$$\underline{\left[ Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset} \right]^{\leq 1}_{\mathcal{Z}}} := \max \left\{ 0, \underline{Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}} - \sqrt{\overline{w}^{>1}_{\mathcal{Z}}} - \overline{w}^{>1}_{\mathcal{Z}} \right\}, \tag{C291}$$

$$\overline{\left[ Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset} \right]^{\leq 1}_{\mathcal{Z}}} := \min \left\{ 1, \overline{Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}} + \sqrt{\overline{w}^{>1}_{\mathcal{Z}}} \right\}. \tag{C292}$$

Similarly, we define the restriction of the test-round yields to the ($\leq 1$)-subspace:

$$\left[ Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} \right]^{\leq 1}_{\mathcal{Z}} := \sum_{k=0}^{d-1} \mathrm{Tr} \left[ \frac{\sigma_k}{d} \Pi^{\leq 1}_{\mathcal{Z}} X^{(\eta_i,\eta_l)}_{\checkmark,\checkmark} \Pi^{\leq 1}_{\mathcal{Z}} \right], \tag{C293}$$

$$\left[ Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} \right]^{\leq 1}_{\mathcal{Z}} := \sum_{k=0}^{d-1} \mathrm{Tr} \left[ \frac{\sigma_k}{d} \Pi^{\leq 1}_{\mathcal{Z}} X^{(\eta_i,\eta_l)}_{\checkmark,\emptyset} \Pi^{\leq 1}_{\mathcal{Z}} \right]. \tag{C294}$$

Then we can obtain tight intervals of existence for such quantities:

$$\underline{\left[ Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} \right]^{\leq 1}_{\mathcal{Z}}} \leq \left[ Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} \right]^{\leq 1}_{\mathcal{Z}} \leq \overline{\left[ Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} \right]^{\leq 1}_{\mathcal{Z}}}, \tag{C295}$$

$$\underline{\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} \leq \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} \leq \overline{\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}, \tag{C296}$$

with

$$\underline{\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} := \max\left\{0, \underline{Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}} - \sqrt{\overline{w}^{>1}_{\mathcal{Z}}} - \overline{w}^{>1}_{\mathcal{Z}}\right\}, \tag{C297}$$

$$\overline{\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} := \min\left\{1, \overline{Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}} + \sqrt{\overline{w}^{>1}_{\mathcal{Z}}}\right\}, \tag{C298}$$

$$\underline{\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} := \max\left\{0, \underline{Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}} - \sqrt{\overline{w}^{>1}_{\mathcal{Z}}} - \overline{w}^{>1}_{\mathcal{Z}}\right\}, \tag{C299}$$

$$\overline{\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} := \min\left\{1, \overline{Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}} + \sqrt{\overline{w}^{>1}_{\mathcal{Z}}}\right\}. \tag{C300}$$

Importantly, we expect the intervals in Eqs. (C286), (C290), (C295), and (C296) to collapse to a single point under nominal conditions since $\mathrm{Tr}[\bar{\sigma}\,\Pi^{>1}_{\mathcal{Z}}] = 0$ if there is no eavesdropper adding photons and the bound $\mathrm{Tr}[\bar{\sigma}\,\Pi^{>1}_{\mathcal{Z}}] \leq \overline{w}^{>1}_{\mathcal{Z}}$ in Eq. (C218) is tight under such conditions.

Having obtained narrow intervals for the test-round yields and bit error rates restricted to the ($\leq 1$)-subspace, we are one step closer to estimating $\Delta_1$ as defined in Eq. (C249). We observe, however, that the definition of $\Delta_1$ restricts the states to the ($\leq 1$)-subspace through the positive-semidefinite operators $M^{\leq 1}_{\mathcal{Z}}$, defined in Eq. (C220) and reported here for clarity,

$$M^{\leq 1}_{\mathcal{Z}} = \sqrt{p_{\checkmark|0}}\,\Pi^0_{\mathcal{Z}} + \sqrt{p_{\checkmark|1}}\,\Pi^1_{\mathcal{Z}}, \tag{C301}$$

rather than through the projectors $\Pi^{\leq 1}_{\mathcal{Z}} = \Pi^0_{\mathcal{Z}} + \Pi^1_{\mathcal{Z}}$. Therefore, we cannot directly use the bounds derived on the restricted test-round yields and bit error rates to compute $\Delta_1$ since the latter lack the prefactors $\sqrt{p_{\checkmark|0}}$ and $\sqrt{p_{\checkmark|1}}$ in their definitions, Eqs. (C293), (C294), (C282), and (C289).

Therefore, to obtain a precise estimation of $\Delta_1$, we need to expand each quantity restricted to the ($\leq 1$)-subspace, namely, Eqs. (C293), (C294), (C282), and (C289), through the equality $\Pi^{\leq 1}_{\mathcal{Z}} = \Pi^0_{\mathcal{Z}} + \Pi^1_{\mathcal{Z}}$ and then individually estimate the three resulting terms. The three terms can then be multiplied by the appropriate prefactor in $\Delta_1$ after our expanding $\Delta_1$ in a similar way through Eq. (C301). We detail this in the following subsection.

### *h. Expanding the test-round yields and bit error rates restricted to the (≤1)-subspace*

Here we expand the expectation values in Eqs. (C293), (C294), (C282), and (C289) through $\Pi^{\leq 1}_{\mathcal{Z}} = \Pi^0_{\mathcal{Z}} + \Pi^1_{\mathcal{Z}}$. We show that they result in three independent terms that can be individually estimated thanks to the different statistics collected by our tuning the TBS.

We start by expanding the test-round yield defined in Eq. (C293). The other test-round yield and bit error rates follow a similar pattern. By using $\Pi^{\leq 1}_{\mathcal{Z}} = \Pi^0_{\mathcal{Z}} + \Pi^1_{\mathcal{Z}}$ and Eq. (C173), we get three terms:

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} = \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0}_{\mathcal{Z}} + \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}} + \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{1}_{\mathcal{Z}}, \tag{C302}$$

where we defined

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0}_{\mathcal{Z}} := \mathrm{Tr}\left[\bar{\sigma}\,\Pi^0_{\mathcal{Z}} X^{(\eta_i,\eta_l)}_{\checkmark,\checkmark}\,\Pi^0_{\mathcal{Z}}\right], \tag{C303}$$

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}} := \mathrm{Tr}\left[\bar{\sigma}\left(\Pi^0_{\mathcal{Z}} X^{(\eta_i,\eta_l)}_{\checkmark,\checkmark}\,\Pi^1_{\mathcal{Z}} + \mathrm{H.c.}\right)\right], \tag{C304}$$

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{1}_{\mathcal{Z}} := \mathrm{Tr}\left[\bar{\sigma}\,\Pi^1_{\mathcal{Z}} X^{(\eta_i,\eta_l)}_{\checkmark,\checkmark}\,\Pi^1_{\mathcal{Z}}\right]. \tag{C305}$$

We note that we can easily derive nontrivial intervals of existence for the three terms in Eq. (C302). In particular, we have (for $\alpha = 0, 1$)

$$0 \leq \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{\alpha}_{\mathcal{Z}} \leq \overline{w}^{\alpha}_{\mathcal{Z}}, \tag{C306}$$

where we used the fact that $X^{(\eta_i,\eta_l)}_{\checkmark,\checkmark} \leq \mathbb{1}$ and the upper bounds in Eqs. (C194) and (C199). By combining Eqs. (C302) and (C306), we obtain an interval for the remaining term:

$$\underline{\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} - (\overline{w}^0_{\mathcal{Z}} + \overline{w}^1_{\mathcal{Z}}) \leq \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}} \leq \overline{\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}. \tag{C307}$$

For each of the terms in Eq. (C302), we use Eq. (C272) combined with Eqs. (C268) and (C155) to recast the terms as follows:

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0}_{\mathcal{Z}} = \mathrm{Tr}_{ab}\left[(\bar{\sigma}\otimes\mathbb{1}_b)\,(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^\dagger_{(\eta_i,\eta_l)}(X_\checkmark)_c \otimes (p_d^{\mathcal{Z}}\Pi^0_{\mathcal{Z}} + \textstyle\sum_{\alpha=1}^{\infty}\Pi^\alpha_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\right], \tag{C308}$$

$$\begin{aligned}\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}} &= \mathrm{Tr}_{ab}\left[(\bar{\sigma}\otimes\mathbb{1}_b)\,(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^\dagger_{(\eta_i,\eta_l)}(X_\checkmark)_c \otimes (p_d^{\mathcal{Z}}\Pi^0_{\mathcal{Z}} + \textstyle\sum_{\alpha=1}^{\infty}\Pi^\alpha_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\right] \\ &\quad + \mathrm{Tr}_{ab}\left[(\bar{\sigma}\otimes\mathbb{1}_b)\,(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^\dagger_{(\eta_i,\eta_l)}(X_\checkmark)_c \otimes (p_d^{\mathcal{Z}}\Pi^0_{\mathcal{Z}} + \textstyle\sum_{\alpha=1}^{\infty}\Pi^\alpha_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\right],\end{aligned} \tag{C309}$$

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{1}_{\mathcal{Z}} = \mathrm{Tr}_{ab}\left[(\bar{\sigma}\otimes\mathbb{1}_b)\,(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^\dagger_{(\eta_i,\eta_l)}(X_\checkmark)_c \otimes (p_d^{\mathcal{Z}}\Pi^0_{\mathcal{Z}} + \textstyle\sum_{\alpha=1}^{\infty}\Pi^\alpha_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\right]. \tag{C310}$$

Then we observe that the unitary action of the TBS, as defined in Eq. (C152), preserves the temporal localization of each photon. In other words, if there are $\zeta$ incoming photons localized in $\mathcal{Z}$ among the two incoming modes, then there must also be $\zeta$ outgoing photons in $\mathcal{Z}$ in the two outgoing modes. Therefore, by recalling that $\mathbb{1} = \sum_\alpha \Pi^\alpha_{\mathcal{Z}}$, we can write

$$\begin{aligned}U_{(\eta_i,\eta_l)} &= \mathbb{1}_c \otimes \mathbb{1}_{c'} U_{(\eta_i,\eta_l)} \mathbb{1}_a \otimes \mathbb{1}_b \\ &= \sum_{\zeta=0}^{\infty}\sum_{\beta=0}^{\zeta}(\Pi^\beta_{\mathcal{Z}})_c \otimes (\Pi^{\zeta-\beta}_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)} \sum_{\alpha=0}^{\zeta}(\Pi^\alpha_{\mathcal{Z}})_a \otimes (\Pi^{\zeta-\alpha}_{\mathcal{Z}})_b,\end{aligned} \tag{C311}$$

where the last expression implements the above observation. We now apply the observation in Eq. (C311) to compute the following quantities appearing in Eq. (C302):

$$U_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b = (\Pi^0_{\mathcal{Z}})_c \otimes (\Pi^0_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b, \tag{C312}$$

$$U_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b = \left[(\Pi^0_{\mathcal{Z}})_c \otimes (\Pi^1_{\mathcal{Z}})_{c'} + (\Pi^1_{\mathcal{Z}})_c \otimes (\Pi^0_{\mathcal{Z}})_{c'}\right] U_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b. \tag{C313}$$

By taking the Hermitian conjugate of the above expressions, we obtain

$$(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^\dagger_{(\eta_i,\eta_l)} = (\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^\dagger_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}})_c \otimes (\Pi^0_{\mathcal{Z}})_{c'}, \tag{C314}$$

$$(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^\dagger_{(\eta_i,\eta_l)} = (\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^\dagger_{(\eta_i,\eta_l)}\left[(\Pi^0_{\mathcal{Z}})_c \otimes (\Pi^1_{\mathcal{Z}})_{c'} + (\Pi^1_{\mathcal{Z}})_c \otimes (\Pi^0_{\mathcal{Z}})_{c'}\right]. \tag{C315}$$

By using Eqs. (C312)–(C315) in Eqs. (C308)–(C310), we rewrite the three terms in Eq. (C302) as follows:

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0}_{\mathcal{Z}} = p_d^{\mathcal{Z}}\,\mathrm{Tr}_{ab}\left[(\bar{\sigma}\otimes \mathbb{1}_b)\,(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^{\dagger}_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}} X_{\checkmark}\,\Pi^0_{\mathcal{Z}})_c \otimes (\Pi^0_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\right], \tag{C316}$$

$$\begin{aligned}\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{1}_{\mathcal{Z}} &= p_d^{\mathcal{Z}}\,\mathrm{Tr}_{ab}\left[(\bar{\sigma}\otimes \mathbb{1}_b)\,(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^{\dagger}_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}} X_{\checkmark}\,\Pi^1_{\mathcal{Z}})_c \otimes (\Pi^0_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\right] \\ &\quad + \mathrm{Tr}_{ab}\left[(\bar{\sigma}\otimes \mathbb{1}_b)\,(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^{\dagger}_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}} X_{\checkmark}\,\Pi^0_{\mathcal{Z}})_c \otimes (\Pi^1_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\right],\end{aligned} \tag{C317}$$

$$\begin{aligned}\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}} &= p_d^{\mathcal{Z}}\,\mathrm{Tr}_{ab}\left[(\bar{\sigma}\otimes \mathbb{1}_b)\,(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^{\dagger}_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}} X_{\checkmark}\,\Pi^1_{\mathcal{Z}})_c \otimes (\Pi^0_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\right] \\ &\quad + p_d^{\mathcal{Z}}\,\mathrm{Tr}_{ab}\left[(\bar{\sigma}\otimes \mathbb{1}_b)\,(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^{\dagger}_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}} X_{\checkmark}\,\Pi^0_{\mathcal{Z}})_c \otimes (\Pi^0_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\right].\end{aligned} \tag{C318}$$

*Remark 6.* We emphasize that $\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}}$ is, in general, not null. The operator $(X_{\checkmark})_c$, representing a detection in the $X$-basis detector and reported in Eq. (C267), may not be diagonal in the eigenbasis $\{\Pi^{\alpha}_{\mathcal{Z}}\}^{\infty}_{\alpha=0}$ of the operator $(Z_{\checkmark})_{c'}$, representing a detection in the $Z$-basis detector and reported in Eq. (C155).

In a similar manner, we expand the other test-round yield in Eq. (C294) as follows:

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} = \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{0}_{\mathcal{Z}} + \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}} + \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{1}_{\mathcal{Z}}, \tag{C319}$$

with intervals of existence given by

$$0 \leq \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\alpha}_{\mathcal{Z}} \leq \overline{w}^{\alpha}_{\mathcal{Z}}, \tag{C320}$$

$$\underline{\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}} - (\overline{w}^{0}_{\mathcal{Z}} + \overline{w}^{1}_{\mathcal{Z}}) \leq \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}} \leq \overline{\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}, \tag{C321}$$

and where Eq. (C269) and the application of the rules in Eqs. (C312)–(C315) leads to

$$\begin{aligned}\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{0}_{\mathcal{Z}} &= \mathrm{Tr}\left[\bar{\sigma}\,\Pi^0_{\mathcal{Z}} X^{(\eta_i,\eta_l)}_{\checkmark,\emptyset}\,\Pi^0_{\mathcal{Z}}\right] \\ &= (1-p_d^{\mathcal{Z}})\,\mathrm{Tr}_{ab}\left[(\bar{\sigma}\otimes \mathbb{1}_b)\,(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^{\dagger}_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}} X_{\checkmark}\,\Pi^0_{\mathcal{Z}})_c \otimes (\Pi^0_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\right],\end{aligned} \tag{C322}$$

$$\begin{aligned}\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{1}_{\mathcal{Z}} &= \mathrm{Tr}\left[\bar{\sigma}\,\Pi^1_{\mathcal{Z}} X^{(\eta_i,\eta_l)}_{\checkmark,\emptyset}\,\Pi^1_{\mathcal{Z}}\right] \\ &= (1-p_d^{\mathcal{Z}})\,\mathrm{Tr}_{ab}\left[(\bar{\sigma}\otimes \mathbb{1}_b)\,(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^{\dagger}_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}} X_{\checkmark}\,\Pi^1_{\mathcal{Z}})_c \otimes (\Pi^0_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\right],\end{aligned} \tag{C323}$$

$$\begin{aligned}\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}} &= \mathrm{Tr}\left[\bar{\sigma}\left(\Pi^0_{\mathcal{Z}} X^{(\eta_i,\eta_l)}_{\checkmark,\emptyset}\Pi^1_{\mathcal{Z}} + \mathrm{H.c.}\right)\right]\\ &= (1-p_d^{\mathcal{Z}})\,\mathrm{Tr}_{ab}\left[(\bar{\sigma}\otimes \mathbb{1}_b)\,(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^\dagger_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}} X_\checkmark \Pi^1_{\mathcal{Z}})_c \otimes (\Pi^0_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\right]\\ &\quad + (1-p_d^{\mathcal{Z}})\,\mathrm{Tr}_{ab}\left[(\bar{\sigma}\otimes \mathbb{1}_b)\,(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^\dagger_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}} X_\checkmark \Pi^0_{\mathcal{Z}})_c \otimes (\Pi^0_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\right].\end{aligned} \tag{C324}$$

We now show that each of the three terms in Eqs. (C302) and (C319) can be estimated by our solving a system of linear equations. To see this, we compute each expectation value forming the three terms in Eqs. (C302) and (C319), bearing in mind that they are repeated in the two expressions. To do so, we use the definition of $U^\dagger_{(\eta_i,\eta_l)}$ given in Eq. (C152) to replace the creation operators $c^\dagger$ and $(c')^\dagger$ with the creation operators $a^\dagger$ and $b^\dagger$. More precisely, we replace the creation operators of only the outer kets and bras in the operators sandwiched by $U^\dagger_{(\eta_i,\eta_l)}$ and $U_{(\eta_i,\eta_l)}$. Our computation starts from the following operator, appearing in Eqs. (C304) and (C324), and uses the explicit expression for $\Pi^\alpha_{\mathcal{Z}}$ given in Eq. (C156):

$$\begin{aligned}&(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^\dagger_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}} X_\checkmark \Pi^1_{\mathcal{Z}})_c \otimes (\Pi^0_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\\ &\quad = \sum_{n,n'=0}^{\infty}\sum_{m=1}^{\infty}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t_1\cdots\mathrm{d}t_n}{n!}\int_{\mathcal{Z}}\mathrm{d}\tau_1\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}\tau_2\cdots\mathrm{d}\tau_m}{(m-1)!}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t'_1\cdots\mathrm{d}t'_{n'}}{n'!}\,\langle 1_{t_1},\ldots,1_{t_n}|X_\checkmark|1_{\tau_1},\ldots,1_{\tau_m}\rangle,\\ &(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^\dagger_{(\eta_i,\eta_l)}(|1_{t_1},\ldots,1_{t_n}\rangle\langle 1_{\tau_1},\ldots,1_{\tau_m}|)_c \otimes (|1_{t'_1},\ldots,1_{t'_{n'}}\rangle\langle 1_{t'_1},\ldots,1_{t'_{n'}}|)_{c'} U_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\\ &\quad = \sum_{n,n'=0}^{\infty}\sum_{m=1}^{\infty}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t_1\cdots\mathrm{d}t_n}{n!}\int_{\mathcal{Z}}\mathrm{d}\tau_1\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}\tau_2\cdots\mathrm{d}\tau_m}{(m-1)!}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t'_1\cdots\mathrm{d}t'_{n'}}{n'!}\,\langle 1_{t_1},\ldots,1_{t_n}|X_\checkmark|1_{\tau_1},\ldots,1_{\tau_m}\rangle,\\ &(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^\dagger_{(\eta_i,\eta_l)} c^\dagger_{t_1}\ldots c^\dagger_{t_n}\otimes c'^\dagger_{t'_1}\ldots c'^\dagger_{t'_{n'}}|\mathrm{vac}\rangle\langle\mathrm{vac}|c_{\tau_1}\ldots c_{\tau_m}\otimes c'_{t'_1}\ldots c'_{t'_{n'}} U_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\\ &\quad = \sum_{n,n'=0}^{\infty}\sum_{m=1}^{\infty}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t_1\cdots\mathrm{d}t_n}{n!}\int_{\mathcal{Z}}\mathrm{d}\tau_1\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}\tau_2\cdots\mathrm{d}\tau_m}{(m-1)!}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t'_1\cdots\mathrm{d}t'_{n'}}{n'!}\,\langle 1_{t_1},\ldots,1_{t_n}|X_\checkmark|1_{\tau_1},\ldots,1_{\tau_m}\rangle\\ &\qquad\times\sqrt{\eta_i}(1-\eta_l)^{n'}(\sqrt{\eta_l})^{n+m-1}\,|1_{t_1},\ldots,1_{t_n},1_{t'_1},\ldots,1_{t'_{n'}}\rangle\langle 1_{\tau_1},\ldots,1_{\tau_m},1_{t'_1},\ldots,1_{t'_{n'}}|_a\otimes|\mathrm{vac}\rangle\langle\mathrm{vac}|_b.\end{aligned} \tag{C325}$$

Similarly, for the other operator appearing in Eqs. (C304) and (C324), we obtain

$$\begin{aligned}&(\Pi^1_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b U^\dagger_{(\eta_i,\eta_l)}(\Pi^1_{\mathcal{Z}} X_\checkmark \Pi^0_{\mathcal{Z}})_c \otimes (\Pi^0_{\mathcal{Z}})_{c'} U_{(\eta_i,\eta_l)}(\Pi^0_{\mathcal{Z}})_a \otimes |\mathrm{vac}\rangle\langle\mathrm{vac}|_b\\ &\quad = \sum_{n,n'=0}^{\infty}\sum_{m=1}^{\infty}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t_1\cdots\mathrm{d}t_n}{n!}\int_{\mathcal{Z}}\mathrm{d}\tau_1\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}\tau_2\cdots\mathrm{d}\tau_m}{(m-1)!}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t'_1\cdots\mathrm{d}t'_{n'}}{n'!}\,\langle 1_{\tau_1},\ldots,1_{\tau_m}|X_\checkmark|1_{t_1},\ldots,1_{t_n}\rangle\\ &\qquad\times\sqrt{\eta_i}(1-\eta_l)^{n'}(\sqrt{\eta_l})^{n+m-1}\,|1_{\tau_1},\ldots,1_{\tau_m},1_{t'_1},\ldots,1_{t'_{n'}}\rangle\langle 1_{t_1},\ldots,1_{t_n},1_{t'_1},\ldots,1_{t'_{n'}}|_a\otimes|\mathrm{vac}\rangle\langle\mathrm{vac}|_b.\end{aligned} \tag{C326}$$

The important point of the last two calculations is the realization that the action of the TBS generates a prefactor $\sqrt{\eta_i}$, such that $\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}}$ and $\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}}$ can be rewritten as

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}} = p_d^{\mathcal{Z}}\sqrt{\eta_i}\,\mathbb{Y}^{0,1}_{\eta_l}, \tag{C327}$$

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{0,1}_{\mathcal{Z}} = (1-p_d^{\mathcal{Z}})\sqrt{\eta_i}\,\mathbb{Y}^{0,1}_{\eta_l} \tag{C328}$$

for some real number $\mathbb{Y}^{0,1}_{\eta_l}$ that mathematically corresponds to

$$\mathbb{Y}^{0,1}_{\eta_l} = \sum_{n,n'=0}^{\infty}\sum_{m=1}^{\infty}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t_1\cdots\mathrm{d}t_n}{n!}\int_{\mathcal{Z}}\mathrm{d}\tau_1\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}\tau_2\cdots\mathrm{d}\tau_m}{(m-1)!}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t'_1\cdots\mathrm{d}t'_{n'}}{n'!}(1-\eta_l)^{n'}(\sqrt{\eta_l})^{n+m-1}$$
$$\times\left(\langle 1_{\tau_1},\ldots,1_{\tau_m}|X_{\checkmark}|1_{t_1},\ldots,1_{t_n}\rangle\langle 1_{t_1},\ldots,1_{t_n},1_{t'_1},\ldots,1_{t'_{n'}}|\bar{\sigma}|1_{\tau_1},\ldots,1_{\tau_m},1_{t'_1},\ldots,1_{t'_{n'}}\rangle+\text{c.c.}\right) \tag{C329}$$

but that, we emphasize, cannot be directly observed experimentally—analogously to the test-round yields restricted by a combination of $\Pi^0_{\mathcal{Z}}$ and $\Pi^1_{\mathcal{Z}}$.

Nevertheless, in a similar manner, we compute the other terms in Eqs. (C302) and (C319) and obtain

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^0_{\mathcal{Z}} = p_d^{\mathcal{Z}}\mathbb{Y}^0_{\eta_l}, \tag{C330}$$
$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^0_{\mathcal{Z}} = (1-p_d^{\mathcal{Z}})\mathbb{Y}^0_{\eta_l} \tag{C331}$$

for a non-negative real number

$$\mathbb{Y}^0_{\eta_l} = \sum_{n,n'=0}^{\infty}\sum_{m=0}^{\infty}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t_1\cdots\mathrm{d}t_n}{n!}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}\tau_1\cdots\mathrm{d}\tau_m}{m!}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t'_1\cdots\mathrm{d}t'_{n'}}{n'!}(1-\eta_l)^{n'}(\sqrt{\eta_l})^{n+m}$$
$$\times\langle 1_{\tau_1},\ldots,1_{\tau_m}|X_{\checkmark}|1_{t_1},\ldots,1_{t_n}\rangle\langle 1_{t_1},\ldots,1_{t_n},1_{t'_1},\ldots,1_{t'_{n'}}|\bar{\sigma}|1_{\tau_1},\ldots,1_{\tau_m},1_{t'_1},\ldots,1_{t'_{n'}}\rangle, \tag{C332}$$

and

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^1_{\mathcal{Z}} = p_d^{\mathcal{Z}}\eta_i\,\mathbb{Y}^{1t}_{\eta_l} + (1-\eta_i)\,\mathbb{Y}^{1r}_{\eta_l}, \tag{C333}$$
$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^1_{\mathcal{Z}} = (1-p_d^{\mathcal{Z}})\eta_i\,\mathbb{Y}^{1t}_{\eta_l}, \tag{C334}$$

for non-negative real numbers

$$\mathbb{Y}^{1t}_{\eta_l} = \sum_{n'=0}^{\infty}\sum_{n,m=1}^{\infty}\int_{\mathcal{Z}}\mathrm{d}t_1\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t_2\cdots\mathrm{d}t_n}{(n-1)!}\int_{\mathcal{Z}}\mathrm{d}\tau_1\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}\tau_2\cdots\mathrm{d}\tau_m}{(m-1)!}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t'_1\cdots\mathrm{d}t'_{n'}}{n'!}(1-\eta_l)^{n'}(\sqrt{\eta_l})^{n+m-2}$$
$$\times\langle 1_{\tau_1},\ldots,1_{\tau_m}|X_{\checkmark}|1_{t_1},\ldots,1_{t_n}\rangle\langle 1_{t_1},\ldots,1_{t_n},1_{t'_1},\ldots,1_{t'_{n'}}|\bar{\sigma}|1_{\tau_1},\ldots,1_{\tau_m},1_{t'_1},\ldots,1_{t'_{n'}}\rangle, \tag{C335}$$
$$\mathbb{Y}^{1r}_{\eta_l} = \sum_{n,m=0}^{\infty}\sum_{n'=1}^{\infty}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t_1\cdots\mathrm{d}t_n}{n!}\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}\tau_1\cdots\mathrm{d}\tau_m}{m!}\int_{\mathcal{Z}}\mathrm{d}t'_1\int_{\overline{\mathcal{Z}}}\frac{\mathrm{d}t'_2\cdots\mathrm{d}t'_{n'}}{(n'-1)!}(1-\eta_l)^{n'-1}(\sqrt{\eta_l})^{n+m}$$
$$\times\langle 1_{\tau_1},\ldots,1_{\tau_m}|X_{\checkmark}|1_{t_1},\ldots,1_{t_n}\rangle\langle 1_{t_1},\ldots,1_{t_n},1_{t'_1},\ldots,1_{t'_{n'}}|\bar{\sigma}|1_{\tau_1},\ldots,1_{\tau_m},1_{t'_1},\ldots,1_{t'_{n'}}\rangle, \tag{C336}$$

where the superscript $t$ ($r$) stands for the fact that the photon localized in $\mathcal{Z}$ is transmitted (reflected) by the TBS.

As already argued, we cannot directly learn the values of $\mathbb{Y}^0_{\eta_l}$, $\mathbb{Y}^{0,1}_{\eta_l}$, $\mathbb{Y}^{1t}_{\eta_l}$, and $\mathbb{Y}^{1r}_{\eta_l}$ from the experiment statistics. However, we know that the sum of Eqs. (C327), (C330), and (C333) [respectively, Eqs. (C328), (C331), and (C334)] is equal to $\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}$ $\left(\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}\right)$, which we managed to tightly bound from above and from below in Eq. (C295) [respectively, Eq. (C296)] in terms of observed statistics. Thus, for the moment, we treat $\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}$ and $\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}$ as

known quantities and write down the following linear system of equations that follows from Eqs. (C302) and (C319):

$$\begin{cases} \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} &= p_d^{\mathcal{Z}}\left(\mathbb{Y}^0_{\eta_l} + \sqrt{\eta_i}\,\mathbb{Y}^{0,1}_{\eta_l} + \eta_i\,\mathbb{Y}^{1t}_{\eta_l}\right) + (1-\eta_i)\,\mathbb{Y}^{1r}_{\eta_l}, \\ \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} &= (1-p_d^{\mathcal{Z}})\left(\mathbb{Y}^0_{\eta_l} + \sqrt{\eta_i}\,\mathbb{Y}^{0,1}_{\eta_l} + \eta_i\,\mathbb{Y}^{1t}_{\eta_l}\right), \end{cases} \tag{C337}$$

where the left-hand sides are known, while the unknowns are the variables $\mathbb{Y}^0_{\eta_l}$, $\mathbb{Y}^{0,1}_{\eta_l}$, $\mathbb{Y}^{1t}_{\eta_l}$, and $\mathbb{Y}^{1r}_{\eta_l}$. Note that the system is composed of pairs of equations like the ones reported, each pair fixed by a choice of $\eta_i$, thus totaling six equations (recall that Bob can select $\eta_i \in \{\eta_\uparrow, \eta_\downarrow, \eta_2\}$). By solving the system of equations for $\mathbb{Y}^0_{\eta_l}$, $\mathbb{Y}^{0,1}_{\eta_l}$, $\mathbb{Y}^{1t}_{\eta_l}$, and $\mathbb{Y}^{1r}_{\eta_l}$, we can deduce the values of each of the three terms in the expansions (C302) and (C319) and use the latter to compute $\Delta_1$.

In a way similar to what is done for the test-round yields, we can expand the test-round bit error rates in Eqs. (C282) and (C289) into three terms:

$$\begin{aligned} \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{\leq 1}_{\mathcal{Z}} &= \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{0}_{\mathcal{Z}} \\ &\quad + \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{0,1}_{\mathcal{Z}} + \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{1}_{\mathcal{Z}}, \end{aligned} \tag{C338}$$

$$\begin{aligned} \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}} &= \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{0}_{\mathcal{Z}} \\ &\quad + \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{0,1}_{\mathcal{Z}} + \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{1}_{\mathcal{Z}}, \end{aligned} \tag{C339}$$

where the first term represents the test-round bit error rate restricted by the projector $\Pi^0_{\mathcal{Z}}$,

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{0}_{\mathcal{Z}} := \sum_{k=0}^{d-1} \mathrm{Tr}\left[\frac{\sigma_k}{d}\Pi^0_{\mathcal{Z}} \sum_{k'\neq k} X^{(\eta_i,\eta_l)}_{k',\checkmark}\Pi^0_{\mathcal{Z}}\right], \tag{C340}$$

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{0}_{\mathcal{Z}} := \sum_{k=0}^{d-1} \mathrm{Tr}\left[\frac{\sigma_k}{d}\Pi^0_{\mathcal{Z}} \sum_{k'\neq k} X^{(\eta_i,\eta_l)}_{k',\emptyset}\Pi^0_{\mathcal{Z}}\right], \tag{C341}$$

while the third term is restricted by $\Pi^1_{\mathcal{Z}}$:

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{1}_{\mathcal{Z}} := \sum_{k=0}^{d-1} \mathrm{Tr}\left[\frac{\sigma_k}{d}\Pi^1_{\mathcal{Z}} \sum_{k'\neq k} X^{(\eta_i,\eta_l)}_{k',\checkmark}\Pi^1_{\mathcal{Z}}\right], \tag{C342}$$

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{1}_{\mathcal{Z}} := \sum_{k=0}^{d-1} \mathrm{Tr}\left[\frac{\sigma_k}{d}\Pi^1_{\mathcal{Z}} \sum_{k'\neq k} X^{(\eta_i,\eta_l)}_{k',\emptyset}\Pi^1_{\mathcal{Z}}\right], \tag{C343}$$

and the second term is restricted by a combination of $\Pi^0_{\mathcal{Z}}$ and $\Pi^1_{\mathcal{Z}}$,

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{0,1}_{\mathcal{Z}} := \sum_{k=0}^{d-1} \mathrm{Tr}\left[\frac{\sigma_k}{d}\left(\Pi^0_{\mathcal{Z}} \sum_{k'\neq k} X^{(\eta_i,\eta_l)}_{k',\checkmark}\Pi^1_{\mathcal{Z}} + \mathrm{H.c.}\right)\right], \tag{C344}$$

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{0,1}_{\mathcal{Z}} := \sum_{k=0}^{d-1} \mathrm{Tr}\left[\frac{\sigma_k}{d}\left(\Pi^0_{\mathcal{Z}} \sum_{k'\neq k} X^{(\eta_i,\eta_l)}_{k',\emptyset}\Pi^1_{\mathcal{Z}} + \mathrm{H.c.}\right)\right]. \tag{C345}$$

Similarly to Eqs. (C320) and (C321), we can derive intervals of existence for each of the above terms:

$$0 \leq \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{\alpha}_{\mathcal{Z}} \leq \overline{w}^{\alpha}_{\mathcal{Z}}, \tag{C346}$$

$$0 \leq \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{\alpha}_{\mathcal{Z}} \leq \overline{w}^{\alpha}_{\mathcal{Z}}, \tag{C347}$$

$$\underline{\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{\leq 1}_{\mathcal{Z}}} - (\overline{w}^0_{\mathcal{Z}} + \overline{w}^1_{\mathcal{Z}}) \leq \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{0,1}_{\mathcal{Z}} \leq \overline{\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{\leq 1}_{\mathcal{Z}}}, \tag{C348}$$

$$\underline{\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}} - (\overline{w}^0_{\mathcal{Z}} + \overline{w}^1_{\mathcal{Z}}) \leq \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{0,1}_{\mathcal{Z}} \leq \overline{\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}. \tag{C349}$$

By performing calculations analogous to those done for the test-round yields, each term in the expansions (C338) and (C339) can be recast as

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{0}_{\mathcal{Z}} = p_d^{\mathcal{Z}}\, \mathbb{E}^{0}_{\eta_l}, \tag{C350}$$

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{0}_{\mathcal{Z}} = (1-p_d^{\mathcal{Z}})\, \mathbb{E}^{0}_{\eta_l}, \tag{C351}$$

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{0,1}_{\mathcal{Z}} = p_d^{\mathcal{Z}} \sqrt{\eta_i}\, \mathbb{E}^{0,1}_{\eta_l}, \tag{C352}$$

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{0,1}_{\mathcal{Z}} = (1-p_d^{\mathcal{Z}}) \sqrt{\eta_i}\, \mathbb{E}^{0,1}_{\eta_l}, \tag{C353}$$

$$\left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{1}_{\mathcal{Z}} = p_d^{\mathcal{Z}} \eta_i\, \mathbb{E}^{1t}_{\eta_l} + (1-\eta_i)\, \mathbb{E}^{1r}_{\eta_l}, \tag{C354}$$

$$\left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{1}_{\mathcal{Z}} = (1-p_d^{\mathcal{Z}}) \eta_i\, \mathbb{E}^{1t}_{\eta_l} \tag{C355}$$

for some real numbers $\mathbb{E}^{0}_{\eta_l}$, $\mathbb{E}^{0,1}_{\eta_l}$, $\mathbb{E}^{1t}_{\eta_l}$, and $\mathbb{E}^{1r}_{\eta_l}$, where again the action of the TBS on the photon localized in $\mathcal{Z}$ is singled out by the factors containing $\eta_i$. Therefore, we can use Eqs. (C350)–(C355) in the expansions (C338) and (C339) to derive the following linear system of equations:

$$\begin{cases} \left[Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark}\right]^{\leq 1}_{\mathcal{Z}} & = p_d^{\mathcal{Z}} \left(\mathbb{E}^{0}_{\eta_l} + \sqrt{\eta_i}\, \mathbb{E}^{0,1}_{\eta_l} + \eta_i\, \mathbb{E}^{1t}_{\eta_l}\right) + (1-\eta_i)\, \mathbb{E}^{1r}_{\eta_l}, \\ \left[Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}} & = (1-p_d^{\mathcal{Z}}) \left(\mathbb{E}^{0}_{\eta_l} + \sqrt{\eta_i}\, \mathbb{E}^{0,1}_{\eta_l} + \eta_i\, \mathbb{E}^{1t}_{\eta_l}\right). \end{cases} \tag{C356}$$

Analogously to the system in Eq. (C337) for the test-round yields, the left-hand sides can be treated as known quantities as they are tightly bounded in Eqs. (C286) and (C290). Hence, we can solve the system for $\mathbb{E}^{0}_{\eta_l}$, $\mathbb{E}^{0,1}_{\eta_l}$, $\mathbb{E}^{1t}_{\eta_l}$, and $\mathbb{E}^{1r}_{\eta_l}$, such that we learn individually each term in the expansions (C338) and (C339).

### *i. Solving the linear systems*

In this section, we solve the linear systems in Eqs. (C337) and (C356). Since the two systems are formally identical, we discuss the solution of the one in Eq. (C337) and apply the result to the other system.

The linear system in Eq. (C337) can be put in the following form, where we selected the second equation three times (for three values of $\eta_i$) and we selected the first equation for $\eta_i = \eta_3$:

$$\begin{pmatrix} \left[Y^{X,\emptyset}_{1,(\eta_1,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} \\ \left[Y^{X,\emptyset}_{1,(\eta_2,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} \\ \left[Y^{X,\emptyset}_{1,(\eta_3,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} \\ \left[Y^{X,\checkmark}_{1,(\eta_3,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} \end{pmatrix} = \Lambda \begin{pmatrix} \mathbb{Y}^{0}_{\eta_l} \\ \mathbb{Y}^{0,1}_{\eta_l} \\ \mathbb{Y}^{1t}_{\eta_l} \\ \mathbb{Y}^{1r}_{\eta_l} \end{pmatrix}, \tag{C357}$$

with the coefficient matrix given by

$$\Lambda := \begin{pmatrix} (1-p_d^{\mathcal{Z}}) & (1-p_d^{\mathcal{Z}})\sqrt{\eta_1} & (1-p_d^{\mathcal{Z}})\eta_1 & 0 \\ (1-p_d^{\mathcal{Z}}) & (1-p_d^{\mathcal{Z}})\sqrt{\eta_2} & (1-p_d^{\mathcal{Z}})\eta_2 & 0 \\ (1-p_d^{\mathcal{Z}}) & (1-p_d^{\mathcal{Z}})\sqrt{\eta_3} & (1-p_d^{\mathcal{Z}})\eta_3 & 0 \\ p_d^{\mathcal{Z}} & p_d^{\mathcal{Z}}\sqrt{\eta_3} & p_d^{\mathcal{Z}}\eta_3 & 1-\eta_3 \end{pmatrix}, \tag{C358}$$

where the three choices of $\eta_i$ correspond to (see Sec III)

$$\eta_1 = \eta_\uparrow, \tag{C359}$$

$$\eta_3 < \eta_2 < \eta_1, \tag{C360}$$

$$\eta_3 = \eta_\downarrow. \tag{C361}$$

The system is solved by one inverting the coefficient matrix. In the protocol's description (Sec. III), we noted that the optimal choice for $\eta_2$ is given by $\eta_2 = \frac{1}{4}(\sqrt{\eta_\uparrow} + \sqrt{\eta_\downarrow})^2$, which maximizes the absolute value of the determinant of $\Lambda$ (and corresponds to the mean of the geometric mean and arithmetic mean of $\eta_\uparrow$ and $\eta_\downarrow$). The solution of the system in Eq. (C337) reads

$$\begin{aligned}\mathbb{Y}^0_{\eta_l} = &\frac{\sqrt{\eta_2\eta_3}}{\left(\sqrt{\eta_1}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_1}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)}\left[Y^{X,\emptyset}_{1,(\eta_1,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} - \frac{\sqrt{\eta_1\eta_3}}{\left(\sqrt{\eta_1}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)}\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} \\ &+ \frac{\sqrt{\eta_1\eta_2}}{\left(\sqrt{\eta_1}-\sqrt{\eta_3}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)}\left[Y^{X,\emptyset}_{1,(\eta_3,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}},\end{aligned} \tag{C362}$$

$$\begin{aligned}\mathbb{Y}^{0,1}_{\eta_l} = &-\frac{\sqrt{\eta_2}+\sqrt{\eta_3}}{\left(\sqrt{\eta_1}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_1}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)}\left[Y^{X,\emptyset}_{1,(\eta_1,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} + \frac{\sqrt{\eta_1}+\sqrt{\eta_3}}{\left(\sqrt{\eta_1}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)}\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} \\ &- \frac{\sqrt{\eta_1}+\sqrt{\eta_2}}{\left(\sqrt{\eta_1}-\sqrt{\eta_3}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)}\left[Y^{X,\emptyset}_{1,(\eta_3,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}},\end{aligned} \tag{C363}$$

$$\begin{aligned}\mathbb{Y}^{1t}_{\eta_l} = &\frac{1}{\left(\sqrt{\eta_1}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_1}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)}\left[Y^{X,\emptyset}_{1,(\eta_1,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} - \frac{1}{\left(\sqrt{\eta_1}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)}\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}} \\ &+ \frac{1}{\left(\sqrt{\eta_1}-\sqrt{\eta_3}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)}\left[Y^{X,\emptyset}_{1,(\eta_3,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}},\end{aligned} \tag{C364}$$

$$\mathbb{Y}^{1r}_{\eta_l} = \frac{\left[Y^{X,\checkmark}_{1,(\eta_3,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}{1-\eta_3} + \frac{\left[Y^{X,\emptyset}_{1,(\eta_3,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}{1-\eta_3}\left(1-\frac{1}{1-p_d^{\mathcal{Z}}}\right). \tag{C365}$$

In the exact same fashion, we solve the linear system in Eq. (C356) and obtain

$$\begin{aligned}\mathbb{E}^0_{\eta_l} = &\frac{\sqrt{\eta_2\eta_3}\left[Y^{X,\emptyset}_{1,(\eta_1,\eta_l)}e_{X,1,(\eta_1,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}{\left(\sqrt{\eta_1}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_1}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)} - \frac{\sqrt{\eta_1\eta_3}\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_l)}e_{X,1,(\eta_2,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}{\left(\sqrt{\eta_1}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)} \\ &+ \frac{\sqrt{\eta_1\eta_2}}{\left(\sqrt{\eta_1}-\sqrt{\eta_3}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)}\left[Y^{X,\emptyset}_{1,(\eta_3,\eta_l)}e_{X,1,(\eta_3,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}},\end{aligned} \tag{C366}$$

$$\begin{aligned}\mathbb{E}^{0,1}_{\eta_l} = &-\frac{\left(\sqrt{\eta_2}+\sqrt{\eta_3}\right)\left[Y^{X,\emptyset}_{1,(\eta_1,\eta_l)}e_{X,1,(\eta_1,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}{\left(\sqrt{\eta_1}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_1}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)} + \frac{\left(\sqrt{\eta_1}+\sqrt{\eta_3}\right)\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_l)}e_{X,1,(\eta_2,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}{\left(\sqrt{\eta_1}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)} \\ &- \frac{\sqrt{\eta_1}+\sqrt{\eta_2}}{\left(\sqrt{\eta_1}-\sqrt{\eta_3}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)}\left[Y^{X,\emptyset}_{1,(\eta_3,\eta_l)}e_{X,1,(\eta_3,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}},\end{aligned} \tag{C367}$$

$$\begin{aligned}\mathbb{E}^{1t}_{\eta_l} = &\frac{\left[Y^{X,\emptyset}_{1,(\eta_1,\eta_l)}e_{X,1,(\eta_1,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}{\left(\sqrt{\eta_1}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_1}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)} - \frac{\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_l)}e_{X,1,(\eta_2,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}{\left(\sqrt{\eta_1}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)} \\ &+ \frac{1}{\left(\sqrt{\eta_1}-\sqrt{\eta_3}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_3}\right)\left(1-p_d^{\mathcal{Z}}\right)}\left[Y^{X,\emptyset}_{1,(\eta_3,\eta_l)}e_{X,1,(\eta_3,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}},\end{aligned} \tag{C368}$$

$$\mathbb{E}^{1r}_{\eta_l} = \frac{\left[Y^{X,\checkmark}_{1,(\eta_3,\eta_l)}e_{X,1,(\eta_3,\eta_l),\checkmark}\right]^{\leq 1}_{\mathcal{Z}}}{1-\eta_3} + \frac{\left[Y^{X,\emptyset}_{1,(\eta_3,\eta_l)}e_{X,1,(\eta_3,\eta_l),\emptyset}\right]^{\leq 1}_{\mathcal{Z}}}{1-\eta_3}\left(1-\frac{1}{1-p_d^{\mathcal{Z}}}\right). \tag{C369}$$

*Remark 7.* With the choices made for $\eta_1$, $\eta_2$, and $\eta_3$ in Eqs. (C359)–(C361), one can verify that the sign of each coefficient, of the restricted test-round yields in Eqs. (C362)–(C365), and of the restricted test-round bit error rates in Eqs. (C362)–(C365), is determined and known.

We observe that the explicit expressions found for the variables $\mathbb{Y}^0_{\eta_l}$, $\mathbb{Y}^{0,1}_{\eta_l}$, $\mathbb{Y}^{1t}_{\eta_l}$, and $\mathbb{Y}^{1r}_{\eta_l}$ ($\mathbb{E}^0_{\eta_l}$, $\mathbb{E}^{0,1}_{\eta_l}$, $\mathbb{E}^{1t}_{\eta_l}$, and $\mathbb{E}^{1r}_{\eta_l}$) are given in terms of the test-round yields (test-round bit error rates) restricted to the $(\leq 1)$-subspace, which are not known exactly but are tightly bounded in Eqs. (C295) and (C296) [Eqs. (C286) and (C290)]. Then, by virtue of Remark 7, we can easily replace the restricted test-round yields (test-round bit error rates) with the respective upper or lower bound, depending on whether the yields (bit error rates) contribute positively or negatively to the phase error rate.

In the following, we use the expressions derived for $\mathbb{Y}^0_{\eta_l}$, $\mathbb{Y}^{0,1}_{\eta_l}$, $\mathbb{Y}^{1t}_{\eta_l}$, and $\mathbb{Y}^{1r}_{\eta_l}$ ($\mathbb{E}^0_{\eta_l}$, $\mathbb{E}^{0,1}_{\eta_l}$, $\mathbb{E}^{1t}_{\eta_l}$, and $\mathbb{E}^{1r}_{\eta_l}$) to obtain the individual values of the three terms in the yields' expansions (C302) and (C319) [bit error rates' expansions (C338) and (C339)]. These are then used to derive an upper bound on $\Delta_1$, where it will become clear how to replace the restricted yields (bit error rates) with their respective bounds from Eqs. (C295) and (C296) [Eqs. (C286) and (C290)].

### *j. Upper bound on* $\Delta_1$*: Part 1*

Here we derive an upper bound on the remaining contribution that is left to be estimated in the phase error rate upper bound, Eq. (C247), namely, $\Delta_1$ given in Eq. (C249). Initially, we aim at calculating an upper bound on the operator $\sum_{k'\neq k}\tilde{X}_{k'}$ appearing in $\Delta_1$, where $\tilde{X}_k$ is the POVM element defined in Eq. (C23) and reported here for clarity:

$$\tilde{X}_k = (\sqrt{X_\checkmark})^{-1} X_k (\sqrt{X_\checkmark})^{-1} \oplus \frac{\mathbb{1}_{X_\checkmark}^{\perp}}{d}, \tag{C370}$$

where both $X_k$ and $X_\checkmark = \sum_k X_k$ are taken from Bob's test measurement, Eq. (C252). According to Eqs. (C268) and (C269), we can obtain an expression for the POVM element $X_k$ of Bob's test measurement, which corresponds to outcome $X_B = k$ in the $X$-basis detector regardless of what happens in the $Z$-basis detector and for the TBS setting $(\eta_\uparrow, \eta_\uparrow)$, as follows:

$$X_k = \langle \mathrm{vac}|_b \, U(\eta_\uparrow)^\dagger (X_k)_c \otimes \mathbb{1}_{c'} U(\eta_\uparrow) \, |\mathrm{vac}\rangle_b \,, \tag{C371}$$

where $U(\eta_\uparrow)$ describes the unitary action of the TBS and where $(X_k)_c$ is given in Eq. (C261). By using Eqs. (C261) in Eq. (C371), we notice that $X_k$ on mode $a$ is just the operator $(X_k)_e$, after letting the incoming mode traverse two lossy elements represented by beam splitters with transmittances $\eta_r$ and $\eta_\uparrow$, respectively. Thus, equivalently, we can compute $X_k$ as resulting from $(X_k)_e$ after one lossy element with a combined transmittance of $\eta_r\eta_\uparrow$, represented by a unitary $U(\eta_r\eta_\uparrow)$ mapping modes $a$ and $b$ to modes $e$ and $f$. Thus, we obtain

$$X_k = \langle \mathrm{vac}|_b \, U^\dagger(\eta_r\eta_\uparrow)(X_k)_e \otimes \mathbb{1}_f \, U(\eta_r\eta_\uparrow) \, |\mathrm{vac}\rangle_b \,. \tag{C372}$$

Then, by analogy with $(X_k)_c$ in Eq. (C261), we can use the result in Eq. (C265) to deduce the final form of $X_k$ on mode $a$:

$$X_k = \sum_{K\in\mathcal{P}(D)\setminus\emptyset} \Pr(k|K) \times \sum_{S\in\mathcal{P}(K)} (p_d^X)^{|K|-|S|}(1-p_d^X)^{d-|K|} \, (M_S^{\geq 1})_a, \tag{C373}$$

where $(M_S^{\geq 1})_a$ is defined as

$$(M_S^{\geq 1})_a = \sum_{\alpha_0,\alpha_1,\ldots,\alpha_{d-1}=0}^{\infty} \Pi_{\mathcal{X}}^{\alpha_0,\alpha_1,\ldots,\alpha_{d-1}} \prod_{s\in S}\left[1-(1-\eta_r\eta_\uparrow)^{\alpha_s}\right] \times \prod_{r\in S^c}(1-\eta_r\eta_\uparrow)^{\alpha_r}. \tag{C374}$$

In a similar manner, we can obtain the expression for $X_\swarrow$, i.e., the POVM element corresponding to a detection in the $X$-basis detector, regardless of what happens in the $Z$-basis detector and for a TBS setting $(\eta_\uparrow, \eta_\uparrow)$. Indeed, from Eq. (C372) we have

$$X_\swarrow = \langle \mathrm{vac}|_b \, U(\eta_r\eta_\uparrow)^\dagger (X_\swarrow)_e \otimes \mathbb{1}_f \, U(\eta_r\eta_\uparrow) \, |\mathrm{vac}\rangle_b \,, \tag{C375}$$

with $(X_\swarrow)_e$ given in Eq. (C260). Then, in analogy with the calculation performed for $(X_\swarrow)_c$ that led to Eq. (C267), from the last expression we obtain the desired expression:

$$X_\swarrow = \sum_{\beta=0}^{\infty}\left[1-(1-p_d^{\mathcal{X}})(1-\eta_r\eta_\uparrow)^\beta\right](\Pi_{\mathcal{X}}^\beta)_a. \tag{C376}$$

From Eq. (C376), we can easily obtain the inverse of its square root:

$$(\sqrt{X_\swarrow})^{-1} = \sum_{\beta=0}^{\infty} \frac{(\Pi_{\mathcal{X}}^\beta)_a}{\sqrt{1-(1-p_d^{\mathcal{X}})(1-\eta_r\eta_\uparrow)^\beta}}, \tag{C377}$$

where we used the fact that the projectors $\Pi_{\mathcal{X}}^\beta$ are orthogonal. Moreover, since $\sum_{\beta=0}^{\infty}\Pi_{\mathcal{X}}^\beta = \mathbb{1}$, we deduce that $X_\swarrow$ has support on the whole Hilbert space:

$$\mathbb{1}_{X_\checkmark} = \mathbb{1}. \tag{C378}$$

To calculate Eq. (C370) we recast the operator in Eq. (C374) as

$$(M_S^{\geq 1})_a = \sum_{\beta=0}^{\infty} \sum_{\substack{\alpha_0,\alpha_1,\ldots,\alpha_{d-1}:\\ \sum_i \alpha_i=\beta}} \Pi_{\mathcal{X}}^{\alpha_0,\alpha_1,\ldots,\alpha_{d-1}} \prod_{s\in S} \left[1-(1-\eta_r\eta_\uparrow)^{\alpha_s}\right] (1-\eta_r\eta_\uparrow)^{\beta-\sum_{s\in S}\alpha_s} \tag{C379}$$

such that, together with Eq. (C377), we get

$$\begin{aligned}
&(\sqrt{X_\checkmark})^{-1}(M_S^{\geq 1})_a(\sqrt{X_\checkmark})^{-1} \\
&= \sum_{\beta=0}^{\infty} \frac{1}{1-(1-p_d^{\mathcal{X}})(1-\eta_r\eta_\uparrow)^{\beta}} \sum_{\substack{\alpha_0,\alpha_1,\ldots,\alpha_{d-1}:\\ \sum_i \alpha_i=\beta}} \Pi_{\mathcal{X}}^{\alpha_0,\alpha_1,\ldots,\alpha_{d-1}} \prod_{s\in S} \left[1-(1-\eta_r\eta_\uparrow)^{\alpha_s}\right] (1-\eta_r\eta_\uparrow)^{\beta-\sum_{s\in S}\alpha_s} \\
&\leq \frac{1}{p_d^{\mathcal{X}}} \Pi_{\mathcal{X}}^0 \, \delta_{S,\emptyset} + \frac{1}{1-(1-p_d^{\mathcal{X}})(1-\eta_r\eta_\uparrow)} \\
&\qquad \times \sum_{\beta=1}^{\infty} \sum_{\substack{\alpha_0,\alpha_1,\ldots,\alpha_{d-1}:\\ \sum_i \alpha_i=\beta}} \Pi_{\mathcal{X}}^{\alpha_0,\alpha_1,\ldots,\alpha_{d-1}} \prod_{s\in S} \left[1-(1-\eta_r\eta_\uparrow)^{\alpha_s}\right] (1-\eta_r\eta_\uparrow)^{\beta-\sum_{s\in S}\alpha_s} \\
&= \left(\frac{1}{p_d^{\mathcal{X}}} - \frac{1}{1-(1-p_d^{\mathcal{X}})(1-\eta_r\eta_\uparrow)}\right) \Pi_{\mathcal{X}}^0 \, \delta_{S,\emptyset} + \frac{1}{1-(1-p_d^{\mathcal{X}})(1-\eta_r\eta_\uparrow)} (M_S^{\geq 1})_a,
\end{aligned} \tag{C380}$$

where in the inequality we pulled out the first term in the sum over $\beta$, noting that it always equals zero except when the set $S$ is empty, and multiplied all the other terms in the sum over $\beta$ by the largest coefficient in the sum. By using the simplifications

$$\frac{1}{p_d^{\mathcal{X}}} - \frac{1}{1-(1-p_d^{\mathcal{X}})(1-\eta_r\eta_\uparrow)} = \frac{\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}{p_d^{\mathcal{X}}[p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})]}, \tag{C381}$$

$$\frac{1}{1-(1-p_d^{\mathcal{X}})(1-\eta_r\eta_\uparrow)} = \frac{1}{p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})} \tag{C382}$$

in Eq. (C380), we obtain

$$(\sqrt{X_\checkmark})^{-1}(M_S^{\geq 1})_a(\sqrt{X_\checkmark})^{-1} \leq \frac{\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}{p_d^{\mathcal{X}}[p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})]} \Pi_{\mathcal{X}}^0 \, \delta_{S,\emptyset} + \frac{1}{p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})} (M_S^{\geq 1})_a. \tag{C383}$$

By using the last expression, together with Eqs. (C373) and (C378), in Eq. (C370), we can derive an upper bound on the following operator that appears in $\Delta_1$:

$$\begin{aligned}
\textstyle\sum_{k'\neq k} \tilde{X}_{k'} &\leq \frac{1}{p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})} \textstyle\sum_{k'\neq k} X_{k'} \\
&\quad + \frac{\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}{p_d^{\mathcal{X}}[p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})]} \sum_{K\in\mathcal{P}(D)\setminus\emptyset} \left(\textstyle\sum_{k'\neq k} \Pr(k'|K)\right) \sum_{S\in\mathcal{P}(K)} (p_d^X)^{|K|-|S|}(1-p_d^X)^{d-|K|} \, \Pi_{\mathcal{X}}^0 \, \delta_{S,\emptyset}.
\end{aligned} \tag{C384}$$

By using Eq. (C254), which implies that $\sum_{k'\neq k} \Pr(k'|K) \leq 1$, we can further simplify the last expression as follows:

$$\textstyle\sum_{k'\neq k} \tilde{X}_{k'} \leq \frac{\sum_{k'\neq k} X_{k'}}{p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})} + \Pi_{\mathcal{X}}^0 \frac{\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}{p_d^{\mathcal{X}}[p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})]} \sum_{K\in\mathcal{P}(D)\setminus\emptyset} (p_d^X)^{|K|}(1-p_d^X)^{d-|K|}. \tag{C385}$$

Now consider that the terms in the sum over the sets $K$ depend only on the cardinality of $K$. Thus, we can turn the sum into a sum over the allowed cardinalities by introducing a binomial coefficient that accounts for the number of different

sets $K$ that can be selected for a given cardinality. This leads to the following chain of equalities:

$$\begin{aligned}\sum_{k'\neq k}\tilde{X}_{k'} &\leq \frac{\sum_{k'\neq k}X_{k'}}{p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}+\Pi^0_{\mathcal{X}}\frac{\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}{p_d^{\mathcal{X}}[p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})]}\sum_{r=1}^{d}\binom{d}{r}(p_d^X)^r(1-p_d^X)^{d-r}\\ &=\frac{1}{p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}\sum_{k'\neq k}X_{k'}+\Pi^0_{\mathcal{X}}\frac{\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}{p_d^{\mathcal{X}}[p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})]}\left[1-(1-p_d^X)^d\right]\\ &=\frac{1}{p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}\sum_{k'\neq k}X_{k'}+\Pi^0_{\mathcal{X}}\frac{\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}{p_d^{\mathcal{X}}[p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})]}p_d^{\mathcal{X}}\\ &=\frac{1}{p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}\sum_{k'\neq k}\left(X^{(\eta_\uparrow,\eta_\uparrow)}_{k',\checkmark}+X^{(\eta_\uparrow,\eta_\uparrow)}_{k',\emptyset}\right)+\frac{\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}{p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}\Pi^0_{\mathcal{X}},\end{aligned}\tag{C386}$$

where in the third line we used Eq. (B3) and in the fourth line we used the definition of Bob's test measurement from Eq. (C252).

By using the operator inequality derived in Eq. (C386) in the expression for $\Delta_1$, Eq. (C249), we obtain the following upper bound on $\Delta_1$:

$$\begin{aligned}\Delta_1 \leq{}& \frac{1}{p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}M^{\leq 1}_{\mathcal{Z}}\sum_{k'\neq k}\left(X^{(\eta_\uparrow,\eta_\uparrow)}_{k',\checkmark}+X^{(\eta_\uparrow,\eta_\uparrow)}_{k',\emptyset}\right)M^{\leq 1}_{\mathcal{Z}}\right]\\ &+\frac{\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}{p_d^{\mathcal{X}}+\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}\mathrm{Tr}\left[\bar{\sigma}M^{\leq 1}_{\mathcal{Z}}\Pi^0_{\mathcal{X}}M^{\leq 1}_{\mathcal{Z}}\right],\end{aligned}\tag{C387}$$

where $M^{\leq 1}_{\mathcal{Z}}$ is given in Eq. (C220) and where we used Eq. (C173). Now the goal is to link the expectation values on the right-hand side of Eq. (C387) to quantities that are observed in the experiment. For the expectation values in the first addend, we expand $M^{\leq 1}_{\mathcal{Z}}$ according to Eq. (C220) and use the definitions in Eq. (C340)–(C345), thus obtaining

$$\begin{aligned}&\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}M^{\leq 1}_{\mathcal{Z}}\sum_{k'\neq k}\left(X^{(\eta_\uparrow,\eta_\uparrow)}_{k',\checkmark}+X^{(\eta_\uparrow,\eta_\uparrow)}_{k',\emptyset}\right)M^{\leq 1}_{\mathcal{Z}}\right]\\ &\quad=p_{\checkmark|0}\left(\left[Y^{X,\checkmark}_{1,(\eta_\uparrow,\eta_\uparrow)}e_{X,1,(\eta_\uparrow,\eta_\uparrow),\checkmark}\right]^0_{\mathcal{Z}}+\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_\uparrow)}e_{X,1,(\eta_\uparrow,\eta_\uparrow),\emptyset}\right]^0_{\mathcal{Z}}\right)\\ &\qquad+\sqrt{p_{\checkmark|0}p_{\checkmark|1}}\left(\left[Y^{X,\checkmark}_{1,(\eta_\uparrow,\eta_\uparrow)}e_{X,1,(\eta_\uparrow,\eta_\uparrow),\checkmark}\right]^{0,1}_{\mathcal{Z}}+\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_\uparrow)}e_{X,1,(\eta_\uparrow,\eta_\uparrow),\emptyset}\right]^{0,1}_{\mathcal{Z}}\right)\\ &\qquad+p_{\checkmark|1}\left(\left[Y^{X,\checkmark}_{1,(\eta_\uparrow,\eta_\uparrow)}e_{X,1,(\eta_\uparrow,\eta_\uparrow),\checkmark}\right]^{1}_{\mathcal{Z}}+\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_\uparrow)}e_{X,1,(\eta_\uparrow,\eta_\uparrow),\emptyset}\right]^{1}_{\mathcal{Z}}\right).\end{aligned}\tag{C388}$$

Now we use the results in Eqs. (C350)–(C355), obtained for the bit error rates restricted by the projectors $\Pi^0_{\mathcal{Z}}$ and $\Pi^1_{\mathcal{Z}}$, to recast the last expression as follows:

$$\begin{aligned}&\sum_{k=0}^{d-1}\mathrm{Tr}\left[\frac{\sigma_k}{d}M^{\leq 1}_{\mathcal{Z}}\sum_{k'\neq k}\left(X^{(\eta_\uparrow,\eta_\uparrow)}_{k',\checkmark}+X^{(\eta_\uparrow,\eta_\uparrow)}_{k',\emptyset}\right)M^{\leq 1}_{\mathcal{Z}}\right]\\ &\quad=p_{\checkmark|0}\mathbb{E}^0_{\eta_\uparrow}+\sqrt{p_{\checkmark|0}p_{\checkmark|1}}\sqrt{\eta_\uparrow}\mathbb{E}^{0,1}_{\eta_\uparrow}+p_{\checkmark|1}\left(\eta_\uparrow\mathbb{E}^{1t}_{\eta_\uparrow}+(1-\eta_\uparrow)\mathbb{E}^{1r}_{\eta_\uparrow}\right),\end{aligned}\tag{C389}$$

where the variables $\mathbb{E}^0_{\eta_\uparrow}$, $\mathbb{E}^{0,1}_{\eta_\uparrow}$, $\mathbb{E}^{1t}_{\eta_\uparrow}$, and $\mathbb{E}^{1r}_{\eta_\uparrow}$ have been obtained in terms of the test-round bit error rates, restricted to the $(\leq 1)$-subspace, in Eqs. (C366)–(C369). We recall that while the test-round bit error rates restricted to the $(\leq 1)$-subspace are not directly observed, they must belong to tight intervals as derived in Eqs. (C286) and (C290).

Therefore, we now replace the variables $\mathbb{E}^0_{\eta_\uparrow}$, $\mathbb{E}^{0,1}_{\eta_\uparrow}$, $\mathbb{E}^{1t}_{\eta_\uparrow}$, and $\mathbb{E}^{1r}_{\eta_\uparrow}$ in Eq. (C389) with the respective upper bounds: $\overline{\mathbb{E}}^0_{\eta_\uparrow}$, $\overline{\mathbb{E}}^{0,1}_{\eta_\uparrow}$, $\overline{\mathbb{E}}^{1t}_{\eta_\uparrow}$, and $\overline{\mathbb{E}}^{1r}_{\eta_\uparrow}$. These bounds are obtained from Eqs. (C366)–(C369) by our substituting each test-round bit error rate, restricted to the $(\leq 1)$-subspace, with the appropriate extremal point from the intervals (C286) and (C290), such that the resulting expression is an upper bound on the original expression. By doing so, we obtain an upper bound on Eq. (C389) that is entirely given in terms of observed quantities and reads

$$\sum_{k=0}^{d-1} \mathrm{Tr}\left[\frac{\sigma_k}{d} M_{\mathcal{Z}}^{\leq 1} \sum_{k' \neq k} \left(X_{k',\checkmark}^{(\eta_\uparrow,\eta_\uparrow)} + X_{k',\emptyset}^{(\eta_\uparrow,\eta_\uparrow)}\right) M_{\mathcal{Z}}^{\leq 1}\right]$$
$$\leq p_{\checkmark|0} \overline{\mathbb{E}}_{\eta_\uparrow}^{0} + \sqrt{p_{\checkmark|0} p_{\checkmark|1}}\, \sqrt{\eta_\uparrow}\, \overline{\mathbb{E}}_{\eta_\uparrow}^{0,1} + p_{\checkmark|1} \left(\eta_\uparrow \overline{\mathbb{E}}_{\eta_\uparrow}^{1t} + (1-\eta_\uparrow) \overline{\mathbb{E}}_{\eta_\uparrow}^{1r}\right), \tag{C390}$$

where in the definitions of the following upper bounds, we replace $\eta_1$ and $\eta_3$ with Eq. (C359) and Eq. (C361), respectively:

$$\overline{\mathbb{E}}_{\eta_\uparrow}^{0} := \min \left\{ \overline{w}_{\mathcal{Z}}^{0}, \frac{\sqrt{\eta_2 \eta_\downarrow} \overline{\left[Y_{1,(\eta_\uparrow,\eta_\uparrow)}^{X,\emptyset} e_{X,1,(\eta_\uparrow,\eta_\uparrow),\emptyset}\right]_{\mathcal{Z}}^{\leq 1}}}{\left(\sqrt{\eta_\uparrow} - \sqrt{\eta_2}\right)\left(\sqrt{\eta_\uparrow} - \sqrt{\eta_\downarrow}\right)\left(1 - p_d^{\mathcal{Z}}\right)} - \frac{\sqrt{\eta_\uparrow \eta_\downarrow} \underline{\left[Y_{1,(\eta_2,\eta_\uparrow)}^{X,\emptyset} e_{X,1,(\eta_2,\eta_\uparrow),\emptyset}\right]_{\mathcal{Z}}^{\leq 1}}}{\left(\sqrt{\eta_\uparrow} - \sqrt{\eta_2}\right)\left(\sqrt{\eta_2} - \sqrt{\eta_\downarrow}\right)\left(1 - p_d^{\mathcal{Z}}\right)} \right.$$
$$\left. + \frac{\sqrt{\eta_\uparrow \eta_2}}{\left(\sqrt{\eta_\uparrow} - \sqrt{\eta_\downarrow}\right)\left(\sqrt{\eta_2} - \sqrt{\eta_\downarrow}\right)\left(1 - p_d^{\mathcal{Z}}\right)} \overline{\left[Y_{1,(\eta_\downarrow,\eta_\uparrow)}^{X,\emptyset} e_{X,1,(\eta_\downarrow,\eta_\uparrow),\emptyset}\right]_{\mathcal{Z}}^{\leq 1}} \right\}, \tag{C391}$$

$$\overline{\mathbb{E}}_{\eta_\uparrow}^{0,1} := \min \left\{ \frac{\overline{\left[Y_{1,(\eta_\uparrow,\eta_\uparrow)}^{X,\emptyset} e_{X,1,(\eta_\uparrow,\eta_\uparrow),\emptyset}\right]_{\mathcal{Z}}^{\leq 1}}}{\left(1 - p_d^{\mathcal{Z}}\right)\sqrt{\eta_\uparrow}}, - \frac{\left(\sqrt{\eta_2} + \sqrt{\eta_\downarrow}\right) \underline{\left[Y_{1,(\eta_\uparrow,\eta_\uparrow)}^{X,\emptyset} e_{X,1,(\eta_\uparrow,\eta_\uparrow),\emptyset}\right]_{\mathcal{Z}}^{\leq 1}}}{\left(\sqrt{\eta_\uparrow} - \sqrt{\eta_2}\right)\left(\sqrt{\eta_\uparrow} - \sqrt{\eta_\downarrow}\right)\left(1 - p_d^{\mathcal{Z}}\right)} \right.$$
$$\left. + \frac{\left(\sqrt{\eta_\uparrow} + \sqrt{\eta_\downarrow}\right) \overline{\left[Y_{1,(\eta_2,\eta_\uparrow)}^{X,\emptyset} e_{X,1,(\eta_2,\eta_\uparrow),\emptyset}\right]_{\mathcal{Z}}^{\leq 1}}}{\left(\sqrt{\eta_\uparrow} - \sqrt{\eta_2}\right)\left(\sqrt{\eta_2} - \sqrt{\eta_\downarrow}\right)\left(1 - p_d^{\mathcal{Z}}\right)} - \frac{\left(\sqrt{\eta_\uparrow} + \sqrt{\eta_2}\right) \underline{\left[Y_{1,(\eta_\downarrow,\eta_\uparrow)}^{X,\emptyset} e_{X,1,(\eta_\downarrow,\eta_\uparrow),\emptyset}\right]_{\mathcal{Z}}^{\leq 1}}}{\left(\sqrt{\eta_\uparrow} - \sqrt{\eta_\downarrow}\right)\left(\sqrt{\eta_2} - \sqrt{\eta_\downarrow}\right)\left(1 - p_d^{\mathcal{Z}}\right)} \right\}, \tag{C392}$$

$$\overline{\mathbb{E}}_{\eta_\uparrow}^{1t} := \min \left\{ \overline{w}_{\mathcal{Z}}^{1}, \frac{\overline{\left[Y_{1,(\eta_\uparrow,\eta_\uparrow)}^{X,\emptyset} e_{X,1,(\eta_\uparrow,\eta_\uparrow),\emptyset}\right]_{\mathcal{Z}}^{\leq 1}}}{\left(\sqrt{\eta_\uparrow} - \sqrt{\eta_2}\right)\left(\sqrt{\eta_\uparrow} - \sqrt{\eta_\downarrow}\right)\left(1 - p_d^{\mathcal{Z}}\right)} - \frac{\underline{\left[Y_{1,(\eta_2,\eta_\uparrow)}^{X,\emptyset} e_{X,1,(\eta_2,\eta_\uparrow),\emptyset}\right]_{\mathcal{Z}}^{\leq 1}}}{\left(\sqrt{\eta_\uparrow} - \sqrt{\eta_2}\right)\left(\sqrt{\eta_2} - \sqrt{\eta_\downarrow}\right)\left(1 - p_d^{\mathcal{Z}}\right)} \right.$$
$$\left. + \frac{1}{\left(\sqrt{\eta_\uparrow} - \sqrt{\eta_\downarrow}\right)\left(\sqrt{\eta_2} - \sqrt{\eta_\downarrow}\right)\left(1 - p_d^{\mathcal{Z}}\right)} \overline{\left[Y_{1,(\eta_\downarrow,\eta_\uparrow)}^{X,\emptyset} e_{X,1,(\eta_\downarrow,\eta_\uparrow),\emptyset}\right]_{\mathcal{Z}}^{\leq 1}} \right\}, \tag{C393}$$

$$\overline{\mathbb{E}}_{\eta_\uparrow}^{1r} := \min \left\{ \overline{w}_{\mathcal{Z}}^{1}, \frac{\overline{\left[Y_{1,(\eta_\downarrow,\eta_\uparrow)}^{X,\checkmark} e_{X,1,(\eta_\downarrow,\eta_\uparrow),\checkmark}\right]_{\mathcal{Z}}^{\leq 1}}}{1 - \eta_\downarrow} - \frac{p_d^{\mathcal{Z}}}{(1-\eta_\downarrow)(1-p_d^{\mathcal{Z}})} \underline{\left[Y_{1,(\eta_\downarrow,\eta_\uparrow)}^{X,\emptyset} e_{X,1,(\eta_\downarrow,\eta_\uparrow),\emptyset}\right]_{\mathcal{Z}}^{\leq 1}} \right\}. \tag{C394}$$

In the last expression, the upper and lower bounds on the test-round bit error rates are reported in Eqs. (C287), (C288), (C291), and (C292). Moreover, we used the intervals of existence in Eqs. (C346)–(C349) to obtain nontrivial ranges for the upper bounds in Eqs. (C391)–(C394). For example, Eq. (C351) combined with the interval (C347) implies the following upper bound:

$$\mathbb{E}_{\eta_\uparrow}^{0} \leq \overline{w}_{\mathcal{Z}}^{0} / (1 - p_d^{\mathcal{Z}}). \tag{C395}$$

However, since the upper bound provided by the interval (C347) is independent of $p_d^{\mathcal{Z}}$ and since $\mathbb{E}_{\eta_\uparrow}^{0}$ does not implicitly depend on $p_d^{\mathcal{Z}}$, we can set $p_d^{\mathcal{Z}} \to 0$ in the upper bound (C395), thereby obtaining the condition in Eq. (C391). The same can be argued for $\mathbb{E}_{\eta_\uparrow}^{1t}$ and $\mathbb{E}_{\eta_\uparrow}^{1r}$. Conversely, the upper bound on $\mathbb{E}_{\eta_\uparrow}^{0,1}$ implied by Eq. (C349) in general depends on $p_d^{\mathcal{Z}}$ and $\eta_\uparrow$; therefore, the two parameters cannot be set to arbitrary values in the denominator of the first term in Eq. (C392).

Similarly to Eq. (C388), we can expand the second expectation value in Eq. (C387) as follows:

$$\begin{aligned}&\mathrm{Tr}\left[\bar{\sigma} M_{\bar{\mathcal{Z}}}^{\leq 1} \Pi_{\mathcal{X}}^{0} M_{\bar{\mathcal{Z}}}^{\leq 1}\right] \\ &= p_{\checkmark|0}\,\mathrm{Tr}\left[\bar{\sigma}\,\Pi_{\mathcal{Z}}^{0}\Pi_{\mathcal{X}}^{0}\Pi_{\mathcal{Z}}^{0}\right] \\ &\quad + \sqrt{p_{\checkmark|0}p_{\checkmark|1}}\,\mathrm{Tr}\left[\bar{\sigma}\left(\Pi_{\mathcal{Z}}^{0}\Pi_{\mathcal{X}}^{0}\Pi_{\mathcal{Z}}^{1} + \mathrm{H.c.}\right)\right] \\ &\quad + p_{\checkmark|1}\,\mathrm{Tr}\left[\bar{\sigma}\,\Pi_{\mathcal{Z}}^{1}\Pi_{\mathcal{X}}^{0}\Pi_{\mathcal{Z}}^{1}\right]. \end{aligned} \tag{C396}$$

The three expectation values on the right-hand side are not directly observed experimentally and can be interpreted as the weights of the average state received by Bob in the subspace with no photons in $\mathcal{X}$ (which is the total set of modes measured by the $X$-basis detector) when restricted by the projectors $\Pi_{\mathcal{Z}}^{0}$ and $\Pi_{\mathcal{Z}}^{1}$. To estimate such quantities, in the following we link them to the test-round yields restricted to the $(\leq 1)$-subspace [Eqs. (C293) and (C294)] through the detector decoy technique [28].

### *k. Detector decoy technique applied on the X-basis detector statistics*

The statistic collected in the test rounds that is required to estimate the three expectation values in Eq. (C396) is the detection probability in the $X$-basis detector, given the TBS setting $(\eta_l, \eta_l)$ and regardless of the measurement outcome in the $Z$-basis detector. This probability is generated by the following POVM element:

$$\begin{aligned}X_{\checkmark}^{(\eta_l,\eta_l)} &:= \sum_{k=0}^{d-1}\left(X_{k,\checkmark}^{(\eta_l,\eta_l)} + X_{k,\emptyset}^{(\eta_l,\eta_l)}\right) \\ &= \langle \mathrm{vac}|_b\, U^{\dagger}(\eta_l)(X_{\checkmark})_c \otimes \mathbb{1}_{c'} U(\eta_l)\,|\mathrm{vac}\rangle_b, \end{aligned} \tag{C397}$$

where in the second equality we used Eqs. (C268) and (C269). By using the same observation made earlier in Eq. (C372) to compute an explicit expression for the POVM element $X_k$ of Bob's test measurement, we can view $X_{\checkmark}^{(\eta_l,\eta_l)}$ as resulting from $(X_{\checkmark})_e$ when preceded by two lossy elements with transmittances $\eta_l$ and $\eta_r$, respectively. Therefore, we can recast the last expression as follows:

$$\begin{aligned}X_{\checkmark}^{(\eta_l,\eta_l)} &= \langle \mathrm{vac}|_b\, U^{\dagger}(\eta_r\eta_l)(X_{\checkmark})_e \otimes \mathbb{1}_f\, U(\eta_r\eta_l)\,|\mathrm{vac}\rangle_b \\ &= \sum_{\beta=0}^{\infty}\left[1-(1-p_d^{\mathcal{X}})(1-\eta_r\eta_l)^{\beta}\right]\Pi_{\mathcal{X}}^{\beta}, \end{aligned} \tag{C398}$$

where in the second equality we used the similar result obtained for $X_{\checkmark}$ in Eq. (C376). From Eq. (C398) we obtain the POVM element corresponding to no detection in the $X$-basis detector with TBS setting $(\eta_l, \eta_l)$:

$$\begin{aligned}X_{\emptyset}^{(\eta_l,\eta_l)} &:= \mathbb{1} - X_{\checkmark}^{(\eta_l,\eta_l)} \\ &= (1-p_d^{\mathcal{X}})\sum_{\beta=0}^{\infty}(1-\eta_r\eta_l)^{\beta}\Pi_{\mathcal{X}}^{\beta}. \end{aligned} \tag{C399}$$

Thus, the probability of no detection in the $X$-basis detector generated by the average state $\bar{\sigma}$ reads

$$\begin{aligned}&1-\left(Y_{1,(\eta_l,\eta_l)}^{X,\checkmark} + Y_{1,(\eta_l,\eta_l)}^{X,\emptyset}\right) \\ &= \mathrm{Tr}\left[\bar{\sigma} X_{\emptyset}^{(\eta_l,\eta_l)}\right] \\ &= (1-p_d^{\mathcal{X}})\sum_{\beta=0}^{\infty}(1-\eta_r\eta_l)^{\beta}\,\mathrm{Tr}\left[\bar{\sigma}\,\Pi_{\mathcal{X}}^{\beta}\right], \end{aligned} \tag{C400}$$

where we used the definition of test-rounds yields in Eqs. (C270) and (C271).

From Eq. (C400) we realize that the expectation values required in Eq. (C396) are not exactly related to the test-round yields, but rather are related to their restrictions in the subspace with zero photons or one photon in $\mathcal{Z}$. By projecting the state in Eq. (C400) through $\Pi_{\mathcal{Z}}^{0}$ or $\Pi_{\mathcal{Z}}^{1}$, we obtain the following expressions, where on the right-hand side we recover the expectation values of Eq. (C396):

$$\begin{aligned}&\mathrm{Tr}[\bar{\sigma}\,\Pi_{\mathcal{Z}}^{0}] - \left(\left[Y_{1,(\eta_l,\eta_l)}^{X,\checkmark}\right]_{\mathcal{Z}}^{0} + \left[Y_{1,(\eta_l,\eta_l)}^{X,\emptyset}\right]_{\mathcal{Z}}^{0}\right) \\ &= (1-p_d^{\mathcal{X}})\sum_{\beta=0}^{\infty}(1-\eta_r\eta_l)^{\beta}\,\mathrm{Tr}\left[\bar{\sigma}\,\Pi_{\mathcal{Z}}^{0}\Pi_{\mathcal{X}}^{\beta}\Pi_{\mathcal{Z}}^{0}\right], \end{aligned} \tag{C401}$$

$$\begin{aligned}&\mathrm{Tr}[\bar{\sigma}\,\Pi_{\mathcal{Z}}^{1}] - \left(\left[Y_{1,(\eta_l,\eta_l)}^{X,\checkmark}\right]_{\mathcal{Z}}^{1} + \left[Y_{1,(\eta_l,\eta_l)}^{X,\emptyset}\right]_{\mathcal{Z}}^{1}\right) \\ &= (1-p_d^{\mathcal{X}})\sum_{\beta=0}^{\infty}(1-\eta_r\eta_l)^{\beta}\,\mathrm{Tr}\left[\bar{\sigma}\,\Pi_{\mathcal{Z}}^{1}\Pi_{\mathcal{X}}^{\beta}\Pi_{\mathcal{Z}}^{1}\right], \end{aligned} \tag{C402}$$

where we used the definitions of the restricted test-round yields in Eqs. (C303) and (C305). We link the yields restricted to the subspace with either zero photons or one photon in $\mathcal{Z}$ to the variables $\mathbb{Y}_{\eta_l}^{0}$, $\mathbb{Y}_{\eta_l}^{1t}$, and $\mathbb{Y}_{\eta_l}^{1r}$ via the relations (C330), (C331), (C333), and (C334). We obtain

$$\begin{aligned}&\mathrm{Tr}[\bar{\sigma}\,\Pi_{\mathcal{Z}}^{0}] - \mathbb{Y}_{\eta_l}^{0} \\ &= (1-p_d^{\mathcal{X}})\sum_{\beta=0}^{\infty}(1-\eta_r\eta_l)^{\beta}\,\mathrm{Tr}\left[\bar{\sigma}\,\Pi_{\mathcal{Z}}^{0}\Pi_{\mathcal{X}}^{\beta}\Pi_{\mathcal{Z}}^{0}\right], \end{aligned} \tag{C403}$$

$$\mathrm{Tr}[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}] - \left[\eta_l \mathbb{Y}^{1t}_{\eta_l} + (1-\eta_l)\mathbb{Y}^{1r}_{\eta_l}\right] = (1-p_d^{\mathcal{X}}) \sum_{\beta=0}^{\infty} (1-\eta_r\eta_l)^\beta \,\mathrm{Tr}\left[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}\Pi^\beta_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right]. \tag{C404}$$

We emphasize that the left-hand sides of the last two equations can be considered, for the moment, to be known quantities. Indeed, the variables $\mathbb{Y}^0_{\eta_l}$, $\mathbb{Y}^{1t}_{\eta_l}$, and $\mathbb{Y}^{1r}_{\eta_l}$ are expressed in terms of the test-round yields restricted to the $(\leq 1)$-subspace via the solutions (C362)–(C365) to the linear system (C337). In turn, the test-round yields restricted to the $(\leq 1)$-subspace are tightly bounded by observed quantities in Eqs. (C295) and (C296). At the same time, the weights of the average state with zero photons or one photon in $\mathcal{Z}$, namely, $\mathrm{Tr}[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}]$ and $\mathrm{Tr}[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}]$, were already bounded in Eqs. (C194), (C199), (C202), and (C204) when we applied the detector decoy technique to the statistics of the $Z$-basis detector.

We can thus use Eqs. (C403) and (C404) to derive an upper bound on the expectation values $\mathrm{Tr}\left[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^0_{\mathcal{Z}}\right]$ and $\mathrm{Tr}\left[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right]$. To this aim, we observe that Eqs. (C403) and (C404) are of the form

$$f_l = \sum_{\beta=0}^{\infty} t_k^\beta x_\beta, \tag{C405}$$

which allows us to apply the detector decoy technique, where we identified

$$f_l = \frac{\mathrm{Tr}[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}] - \mathbb{Y}^0_{\eta_l}}{1-p_d^{\mathcal{X}}} \quad \text{or} \quad f_l = \frac{\mathrm{Tr}[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}] - \left[\eta_l \mathbb{Y}^{1t}_{\eta_l} + (1-\eta_l)\mathbb{Y}^{1r}_{\eta_l}\right]}{1-p_d^{\mathcal{X}}}, \tag{C406}$$

$$t_k = 1-\eta_r\eta_l, \tag{C407}$$

$$x_\beta = \mathrm{Tr}\left[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}\Pi^\beta_{\mathcal{X}}\Pi^0_{\mathcal{Z}}\right] \quad \text{or} \quad x_\beta = \mathrm{Tr}\left[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}\Pi^\beta_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right], \tag{C408}$$

from which we deduce the following conditions on $x_\beta$:

$$x_\beta \geq 0, \tag{C409}$$

$$\sum_{\beta=0}^{\infty} x_\beta = C, \text{ with } C = \mathrm{Tr}[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}] \text{ or } C = \mathrm{Tr}[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}]. \tag{C410}$$

We now apply the detector decoy technique to derive an upper bound on $x_0$, and thereby on two of the expectation values in Eq. (C396). We recall that $\eta_1 = \eta_\uparrow$ and $\eta_3 = \eta_\downarrow$ (see Sec. III). From Eqs. (C405) and (C410) we obtain the following system of inequalities:

$$\begin{aligned}
&\begin{cases} f_3 \leq x_0 + t_3 x_1 + t_3^2(C - x_0 - x_1), \\ f_1 \geq x_0 + t_1 x_1 \end{cases} \\
\Rightarrow\ &\begin{cases} x_1 \geq \dfrac{f_3 - x_0(1-t_3^2) - Ct_3^2}{t_3(1-t_3)}, \\ x_0 + t_1 \dfrac{f_3 - x_0(1-t_3^2) - Ct_3^2}{t_3(1-t_3)} \leq f_1 \end{cases} \\
\Rightarrow\ &\begin{cases} x_1 \geq \dfrac{f_3 - x_0(1-t_3^2) - Ct_3^2}{t_3(1-t_3)}, \\ x_0\left[1 - \dfrac{t_1(1+t_3)}{t_3}\right] \leq f_1 - t_1 \dfrac{f_3 - Ct_3^2}{t_3(1-t_3)}, \end{cases}
\end{aligned} \tag{C411}$$

where in the second step we used the lower bound on $x_1$ in the second inequality. From the bottom inequality in Eq. (C411), we can derive an upper bound on $x_0$ provided that its coefficient is positive. We thus require that

$$\begin{aligned}
&1 - t_1\frac{1+t_3}{t_3} > 0 && \text{(C412)}\\
\iff\ &t_3 - t_1(1+t_3) > 0 && \text{(C413)}\\
\iff\ &t_3(1-t_1) > t_1 && \text{(C414)}\\
\iff\ &(1-\eta_\downarrow\eta_r)\eta_\uparrow\eta_r > 1-\eta_\uparrow\eta_r && \text{(C415)}\\
\iff\ &-\eta_r^2(\eta_\downarrow\eta_\uparrow) + 2\eta_r\eta_\uparrow - 1 > 0 && \text{(C416)}\\
\iff\ &\eta_r > \frac{1-\sqrt{1-\frac{\eta_\downarrow}{\eta_\uparrow}}}{\eta_\downarrow}, && \text{(C417)}
\end{aligned}$$

which is indeed satisfied since we assumed that the condition in Eq. (10) is satisfied. Then the upper bound on $x_0$ follows from the bottom inequality in Eq. (C411) and reads

$$x_0 \leq \frac{t_3 f_1 - t_1 f_3 + t_3^2(Ct_1 - f_1)}{(1-t_3)[t_3 - t_1(1+t_3)]}. \tag{C418}$$

By substituting the original variables through Eqs. (C406), (C407), and (C408), we obtain the desired upper bound on the weight of the state in the subspace with no photons in $\mathcal{X}$ and in $\mathcal{Z}$:

$$
\begin{aligned}
&\mathrm{Tr}\left[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^0_{\mathcal{Z}}\right]\\
&\leq \frac{(1-\eta_\uparrow\eta_r)\mathbb{Y}^0_{\eta_\downarrow} - (1-\eta_\downarrow\eta_r)\mathbb{Y}^0_{\eta_\uparrow} + \mathrm{Tr}[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}](\eta_\uparrow-\eta_\downarrow)\eta_r + (1-\eta_\downarrow\eta_r)^2\left\{\mathbb{Y}^0_{\eta_\uparrow} - \mathrm{Tr}[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}][p_d^{\mathcal{X}} + \eta_\uparrow\eta_r(1-p_d^{\mathcal{X}})]\right\}}{\eta_\downarrow\eta_r(1-p_d^{\mathcal{X}})(2\eta_\uparrow\eta_r - 1 - \eta_r^2\eta_\uparrow\eta_\downarrow)}\\
&= \frac{(1-\eta_\uparrow\eta_r)\mathbb{Y}^0_{\eta_\downarrow} - \eta_\downarrow\eta_r(1-\eta_\downarrow\eta_r)\mathbb{Y}^0_{\eta_\uparrow} - \mathrm{Tr}[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}]p_d^{\mathcal{X}}(1-\eta_\uparrow\eta_r)(1-\eta_\downarrow\eta_r)^2}{\eta_\downarrow\eta_r(1-p_d^{\mathcal{X}})(2\eta_\uparrow\eta_r - 1 - \eta_r^2\eta_\uparrow\eta_\downarrow)} + \frac{\mathrm{Tr}[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}]}{1-p_d^{\mathcal{X}}}\\
&\leq \overline{\left[w^0_{\mathcal{X}}\right]^0_{\mathcal{Z}}},
\end{aligned}
\tag{C419}
$$

where in the third line we replaced $\mathrm{Tr}[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}]$ with its upper bound or lower bound ($\overline{w}^0_{\mathcal{Z}}$ or $\underline{w}^0_{\mathcal{Z}}$, respectively), such that the resulting expression is still an upper bound of the left-hand side. For the same reason, we defined an upper bound and a lower bound of the variable $\mathbb{Y}^0_{\eta_l}$ starting from its expression in Eq. (C362):

$$
\begin{aligned}
\overline{\mathbb{Y}}^0_{\eta_l} := \min\Bigg\{&\overline{w}^0_{\mathcal{Z}}, \frac{\sqrt{\eta_2\eta_\downarrow}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\overline{\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}\\
&- \frac{\sqrt{\eta_\uparrow\eta_\downarrow}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\underline{\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}\\
&+ \frac{\sqrt{\eta_\uparrow\eta_2}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\overline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}\Bigg\},
\end{aligned}
\tag{C420}
$$

$$
\begin{aligned}
\underline{\mathbb{Y}}^0_{\eta_l} := \max\Bigg\{&0, \frac{\sqrt{\eta_2\eta_\downarrow}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\underline{\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}\\
&- \frac{\sqrt{\eta_\uparrow\eta_\downarrow}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\overline{\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}\\
&+ \frac{\sqrt{\eta_\uparrow\eta_2}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\underline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_l)}\right]^{\leq 1}_{\mathcal{Z}}}\Bigg\},
\end{aligned}
\tag{C421}
$$

respectively, where the upper and lower bounds on the test-round yields in the above formulas are reported in Eqs. (C297), (C298), (C299), and (C300). Note that the nontrivial minimization (maximization) in Eq. (C420) [Eq. (C421)] is obtained from the combination of Eq. (C331) with Eq. (C320), similarly to what was done for $\overline{\mathbb{E}}^0_{\eta_\uparrow}$ in Eq. (C391). In the end, we obtain

$$
\overline{\left[w^0_{\mathcal{X}}\right]^0_{\mathcal{Z}}} := \min\left\{\overline{w}^0_{\mathcal{Z}}, \frac{(1-\eta_\uparrow\eta_r)\overline{\mathbb{Y}}^0_{\eta_\downarrow} - \eta_\downarrow\eta_r(1-\eta_\downarrow\eta_r)\underline{\mathbb{Y}}^0_{\eta_\uparrow} - \underline{w}^0_{\mathcal{Z}}p_d^{\mathcal{X}}(1-\eta_\uparrow\eta_r)(1-\eta_\downarrow\eta_r)^2}{\eta_\downarrow\eta_r(1-p_d^{\mathcal{X}})(2\eta_\uparrow\eta_r - 1 - \eta_r^2\eta_\uparrow\eta_\downarrow)} + \frac{\overline{w}^0_{\mathcal{Z}}}{1-p_d^{\mathcal{X}}}\right\},
\tag{C422}
$$

where $\overline{\mathbb{Y}}^0_{\eta_l}$ and $\underline{\mathbb{Y}}^0_{\eta_l}$ are given in Eqs. (C420) and (C421), while $\overline{w}^0_{\mathcal{Z}}$ and $\underline{w}^0_{\mathcal{Z}}$ are given in Eqs. (C195) and (C204).

In a similar manner, by substituting the original variables back into Eq. (C418), we obtain the desired upper bound on the weight of the state in the subspace with no photons in $\mathcal{X}$ and one photon in $\mathcal{Z}$:

$$
\begin{aligned}
\mathrm{Tr}\left[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right] \leq\ &\frac{(1-\eta_\uparrow\eta_r)\left[\eta_\downarrow\mathbb{Y}^{1t}_{\eta_\downarrow} + (1-\eta_\downarrow)\mathbb{Y}^{1r}_{\eta_\downarrow}\right] - \eta_\downarrow\eta_r(1-\eta_\downarrow\eta_r)\left[\eta_\uparrow\mathbb{Y}^{1t}_{\eta_\uparrow} + (1-\eta_\uparrow)\mathbb{Y}^{1r}_{\eta_\uparrow}\right]}{\eta_\downarrow\eta_r(1-p_d^{\mathcal{X}})(2\eta_\uparrow\eta_r - 1 - \eta_r^2\eta_\uparrow\eta_\downarrow)}\\
&- \frac{\mathrm{Tr}[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}]p_d^{\mathcal{X}}(1-\eta_\uparrow\eta_r)(1-\eta_\downarrow\eta_r)^2}{\eta_\downarrow\eta_r(1-p_d^{\mathcal{X}})(2\eta_\uparrow\eta_r - 1 - \eta_r^2\eta_\uparrow\eta_\downarrow)} + \frac{\mathrm{Tr}[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}]}{1-p_d^{\mathcal{X}}}\\
\leq\ &\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}},
\end{aligned}
\tag{C423}
$$

where in the second inequality we replaced $\mathrm{Tr}[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}]$ with its upper bound or lower bound ($\overline{w}^1_{\mathcal{Z}}$ or $\underline{w}^1_{\mathcal{Z}}$, respectively) and introduced upper and lower bounds on the variables $\mathbb{Y}^{1t}_{\eta_l}$ and $\mathbb{Y}^{1r}_{\eta_l}$, starting from their expressions in Eqs. (C364) and (C365). In this way, we obtain

$$\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}} := \min\left\{\overline{w}^1_{\mathcal{Z}}, \frac{(1-\eta_\uparrow\eta_r)\left[\eta_\downarrow\overline{\mathbb{Y}}^{1t}_{\eta_\downarrow}+(1-\eta_\downarrow)\overline{\mathbb{Y}}^{1r}_{\eta_\downarrow}\right]-\eta_\downarrow\eta_r(1-\eta_\downarrow\eta_r)\left[\eta_\uparrow\underline{\mathbb{Y}}^{1t}_{\eta_\uparrow}+(1-\eta_\uparrow)\underline{\mathbb{Y}}^{1r}_{\eta_\uparrow}\right]}{\eta_\downarrow\eta_r(1-p_d^{\mathcal{X}})(2\eta_\uparrow\eta_r-1-\eta_r^2\eta_\uparrow\eta_\downarrow)}\right.$$
$$\left.-\frac{\underline{w}^1_{\mathcal{Z}}p_d^{\mathcal{X}}(1-\eta_\uparrow\eta_r)(1-\eta_\downarrow\eta_r)^2}{\eta_\downarrow\eta_r(1-p_d^{\mathcal{X}})(2\eta_\uparrow\eta_r-1-\eta_r^2\eta_\uparrow\eta_\downarrow)}+\frac{\overline{w}^1_{\mathcal{Z}}}{1-p_d^{\mathcal{X}}}\right\}, \tag{C424}$$

where $\overline{\mathbb{Y}}^{1t}_{\eta_l}$, $\overline{\mathbb{Y}}^{1r}_{\eta_l}$, $\underline{\mathbb{Y}}^{1t}_{\eta_l}$, and $\underline{\mathbb{Y}}^{1r}_{\eta_l}$ are defined as

$$\overline{\mathbb{Y}}^{1t}_{\eta_l} := \min\left\{\overline{w}^1_{\mathcal{Z}}, \frac{\overline{\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_l)}\right]^{\le 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}-\frac{\underline{\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_l)}\right]^{\le 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\right.$$
$$\left.+\frac{\overline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_l)}\right]^{\le 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\right\}, \tag{C425}$$

$$\overline{\mathbb{Y}}^{1r}_{\eta_l} := \min\left\{\overline{w}^1_{\mathcal{Z}}, \frac{1}{1-\eta_\downarrow}\overline{\left[Y^{X,\checkmark}_{1,(\eta_\downarrow,\eta_l)}\right]^{\le 1}_{\mathcal{Z}}}-\frac{p_d^{\mathcal{Z}}}{(1-\eta_\downarrow)(1-p_d^{\mathcal{Z}})}\underline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_l)}\right]^{\le 1}_{\mathcal{Z}}}\right\}, \tag{C426}$$

$$\underline{\mathbb{Y}}^{1t}_{\eta_l} := \max\left\{0, \frac{\underline{\left[Y^{X,\emptyset}_{1,(\eta_\uparrow,\eta_l)}\right]^{\le 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}-\frac{\overline{\left[Y^{X,\emptyset}_{1,(\eta_2,\eta_l)}\right]^{\le 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_2}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\right.$$
$$\left.+\frac{\underline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_l)}\right]^{\le 1}_{\mathcal{Z}}}}{\left(\sqrt{\eta_\uparrow}-\sqrt{\eta_\downarrow}\right)\left(\sqrt{\eta_2}-\sqrt{\eta_\downarrow}\right)\left(1-p_d^{\mathcal{Z}}\right)}\right\}, \tag{C427}$$

$$\underline{\mathbb{Y}}^{1r}_{\eta_l} := \max\left\{0, \frac{1}{1-\eta_\downarrow}\underline{\left[Y^{X,\checkmark}_{1,(\eta_\downarrow,\eta_l)}\right]^{\le 1}_{\mathcal{Z}}}-\frac{p_d^{\mathcal{Z}}}{(1-\eta_\downarrow)(1-p_d^{\mathcal{Z}})}\overline{\left[Y^{X,\emptyset}_{1,(\eta_\downarrow,\eta_l)}\right]^{\le 1}_{\mathcal{Z}}}\right\}, \tag{C428}$$

while $\overline{w}^1_{\mathcal{Z}}$ and $\underline{w}^1_{\mathcal{Z}}$ are given in Eqs. (C200) and (C202).

After having obtained the upper bounds in Eqs. (C419) and (C423), we now focus on deriving an upper bound on the remaining expectation value in Eq. (C396), namely, $\mathrm{Tr}\left[\bar{\sigma}\,(\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}+\mathrm{H.c.})\right]$. To this aim, we define

$$z := \mathrm{Tr}\left[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right] \tag{C429}$$

such that the expectation value of interest can be bounded as follows:

$$\mathrm{Tr}\left[\bar{\sigma}\,(\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}+\mathrm{H.c.})\right] = z+z^* = 2\mathrm{Re}(z) \le 2|z| = 2\left|\mathrm{Tr}\left[\bar{\sigma}\,\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right]\right|. \tag{C430}$$

We can use the Cauchy-Schwarz inequality in the following form:

$$\left|\mathrm{Tr}[A^\dagger B]\right| \le \sqrt{\mathrm{Tr}[A^\dagger A]\,\mathrm{Tr}[B^\dagger B]}, \tag{C431}$$

where we choose $A = \sqrt{\bar{\sigma}}$ and $B = \Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\sqrt{\bar{\sigma}}$. We obtain

$$\mathrm{Tr}\left[\bar{\sigma}\left(\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}} + \mathrm{H.c.}\right)\right] \leq 2\sqrt{\mathrm{Tr}\left[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right]} \tag{C432}$$

$$\leq 2\sqrt{\mathrm{Tr}\left[\bar{\sigma}\,\Pi^1_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}}\right]}, \tag{C433}$$

where we used the fact that $\Pi^0_{\mathcal{Z}} \leq \mathbb{1}$. Finally, we use the bound already established in Eq. (C423) and obtain the bound on the remaining expectation value:

$$\mathrm{Tr}\left[\bar{\sigma}\left(\Pi^0_{\mathcal{Z}}\Pi^0_{\mathcal{X}}\Pi^1_{\mathcal{Z}} + \mathrm{H.c.}\right)\right] \leq 2\left(\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}\right)^{\frac{1}{2}}. \tag{C434}$$

### *l. Upper bound on* $\boldsymbol{\Delta_1}$*: Part 2*

We can now conclude the derivation of the upper bound on $\Delta_1$, which appears in the phase error rate upper bound, Eq. (C247). In particular, we use the bounds obtained with the detector decoy technique, namely, Eqs. (C419), (C423), and (C434), to obtain an upper bound on Eq. (C396). By using this result with Eq. (C390) in Eq. (C387), we obtain the final expression for the upper bound on $\Delta_1$:

$$\begin{aligned}\Delta_1 \leq{}& \frac{1}{p_d^{\mathcal{X}} + \eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}\left[p_{\checkmark|0}\overline{\mathbb{E}}^0_{\eta_\uparrow} + \sqrt{p_{\checkmark|0}p_{\checkmark|1}}\sqrt{\eta_\uparrow}\overline{\mathbb{E}}^{0,1}_{\eta_\uparrow} + p_{\checkmark|1}\left(\eta_\uparrow\overline{\mathbb{E}}^{1t}_{\eta_\uparrow} + (1-\eta_\uparrow)\overline{\mathbb{E}}^{1r}_{\eta_\uparrow}\right)\right] \\ &+ \frac{\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}{p_d^{\mathcal{X}} + \eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}\left[p_{\checkmark|0}\overline{\left[w^0_{\mathcal{X}}\right]^0_{\mathcal{Z}}} + 2\sqrt{p_{\checkmark|0}p_{\checkmark|1}}\left(\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}\right)^{\frac{1}{2}} + p_{\checkmark|1}\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}\right].\end{aligned} \tag{C435}$$

### *m. Upper bound on the phase error rate*

By using Eq. (C435) in Eq. (C247), we obtain the desired upper bound on the phase error rate, given in terms of quantities that are estimated with the decoy-state method:

$$\tilde{e}_{X,1} \leq \overline{\tilde{e}_{X,1}}, \tag{C436}$$

with

$$\begin{aligned}\overline{\tilde{e}_{X,1}} :={}& \frac{1}{\underline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}[p_d^{\mathcal{X}} + \eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})]}\left[p_{\checkmark|0}\overline{\mathbb{E}}^0_{\eta_\uparrow} + \sqrt{p_{\checkmark|0}p_{\checkmark|1}}\sqrt{\eta_\uparrow}\overline{\mathbb{E}}^{0,1}_{\eta_\uparrow} + p_{\checkmark|1}\left(\eta_\uparrow\overline{\mathbb{E}}^{1t}_{\eta_\uparrow} + (1-\eta_\uparrow)\overline{\mathbb{E}}^{1r}_{\eta_\uparrow}\right)\right] \\ &+ \frac{\eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})}{\underline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}[p_d^{\mathcal{X}} + \eta_r\eta_\uparrow(1-p_d^{\mathcal{X}})]}\left[p_{\checkmark|0}\overline{\left[w^0_{\mathcal{X}}\right]^0_{\mathcal{Z}}} + 2\sqrt{p_{\checkmark|0}p_{\checkmark|1}}\left(\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}\right)^{\frac{1}{2}} + p_{\checkmark|1}\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}\right] \\ &+ \frac{1}{\underline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}}\left(\overline{\Delta_2} + \overline{w}^{>1}_{\mathcal{Z}}\right),\end{aligned} \tag{C437}$$

where $\overline{w}^{>1}_{\mathcal{Z}}$, $\overline{\left[w^0_{\mathcal{X}}\right]^0_{\mathcal{Z}}}$, and $\overline{\left[w^0_{\mathcal{X}}\right]^1_{\mathcal{Z}}}$ are given in Eqs. (C218), (C422), and (C424), respectively, while $\overline{\mathbb{E}}^0_{\eta_\uparrow}$, $\overline{\mathbb{E}}^{0,1}_{\eta_\uparrow}$, $\overline{\mathbb{E}}^{1t}_{\eta_\uparrow}$, and $\overline{\mathbb{E}}^{1r}_{\eta_\uparrow}$ are given in Eqs. (C391)–(C394). Finally, $p_{\checkmark|0}$, $p_{\checkmark|1}$, $\eta_r$, and $\overline{\Delta_2}$ are given in Eqs. (C182), (C183), (C154), and (C248), respectively. The derivation of the bound in Eq. (C437) concludes this subsection.

We observe that all the quantities appearing in Eq. (C437) are either input parameters or expressed in terms of bounds derived with the decoy-state method. In particular, Eq. (C437) contains bounds on the one-photon $Z$-basis yields ($Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}$, $Y^Z_{1,(\eta_\uparrow,\eta_\uparrow)}$), but also indirectly contains bounds on the test-round yields ($Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}$, $Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}$) through Eqs. (C297)–(C300) and on the products between the test-round yields and bit error rates ($Y^{X,\emptyset}_{1,(\eta_i,\eta_\uparrow)}e_{X,1,(\eta_i,\eta_\uparrow),\emptyset}$, $Y^{X,\checkmark}_{1,(\eta_i,\eta_\uparrow)}e_{X,1,(\eta_i,\eta_\uparrow),\checkmark}$) through Eqs. (C287), (C288), (C291), and (C292). Such bounds on the yields and on the bit error rates are obtained with standard procedures of the decoy-state method, as shown in Appendix D.

### 5. Secret key rate

In this subsection we complete the security proof of Protocol 1.

We combine the upper bound obtained on the phase error rate (C436) with the entropy bound (C87) to derive the following bound on the entropy of interest:

$$H(Z_A|E)_{\rho|1,\Omega_Z} \geq \log_2 \frac{1}{c} - u(\overline{\tilde{e}_{X,1}}), \tag{C438}$$

where we used the fact that $u(x)$ in Eq. (20) is a monotonically nondecreasing function. We now use Eq. (C438) in Eq. (C56), together with Eqs. (C47) and (5), to derive the following lower bound on the first entropy that appears in the DW rate (C3):

$$H(Z_A|I_A E)_{\rho|\Omega_Z} \geq \sum_{\mu_j \in \mathcal{S}} \frac{p_{\mu_j}}{\Pr(Z_B \neq \emptyset|\Gamma_Z)} \left\{ e^{-\mu_j} \underline{Y^Z_{0,(\eta_\downarrow,\eta_\downarrow)}} \log_2 d + e^{-\mu_j} \mu_j \underline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}} \left[ \log_2 \frac{1}{c} - u(\overline{\tilde{e}_{X,1}}) \right] \right\}, \tag{C439}$$

where we replaced the yields by their lower bounds obtained with the decoy-state method (see Appendix D).

Finally, we use the lower bound in Eq. (C439) and the upper bound in Eq. (C33) in the DW rate (C3), together with Eq. (C4), to obtain the following lower bound on the asymptotic key rate of the protocol:

$$r \geq p_Z^2 \sum_{j=1}^{3} p_{\mu_j} \left\{ e^{-\mu_j} \underline{Y^Z_{0,(\eta_\downarrow,\eta_\downarrow)}} \log_2 d + e^{-\mu_j} \mu_j \underline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}} \left[ \log_2 \frac{1}{c} - u(\overline{\tilde{e}_{X,1}}) \right] - G^Z_{\mu_j,(\eta_\downarrow,\eta_\downarrow)} u(Q_{Z,\mu_j}) \right\}. \tag{C440}$$

This coincides with the key rate provided in the protocol's description, Eq. (17), thereby concluding the security proof.

## APPENDIX D: DECOY-STATE METHOD

In this appendix, we provide upper and lower bounds on zero-photon and one-photon yields and bit error rates, following the standard procedures of the decoy-state method. Such bounds are required by the phase error rate upper bound, Eq. (B1), as well as in the final expression for the protocol's key rate (17). Moreover, we provide bounds on specific linear combinations of one-photon yields, which appear in Eqs. (B5)–(B9).

### 1. Standard equations of the decoy-state method

We recall from Sec. III that Alice prepares WCPs with three different intensities: $\mathcal{S} = \{\mu_1, \mu_2, \mu_3\}$, with $\mu_1 > \mu_2 + \mu_3$ and $\mu_2 > \mu_3 \geq 0$ . The parties use all three intensities both to generate the key and to derive the decoy bounds. The equalities on which the decoy-state method relies relate the unobserved yields to the observed gains. For instance, by definition (11), the $Z$-basis gain is the probability that Bob has a detection in the $Z$-basis detector, given that Alice sent one of the $Z$-basis states with intensity $\mu_j$ and that Bob chose the TBS setting $(\eta_l, \eta_l)$, and can be expressed as follows:

$$\begin{aligned} G^Z_{\mu_j,(\eta_l,\eta_l)} &= \Pr(Z_B \neq \emptyset | T = Z, I_A = \mu_j, (\eta_l, \eta_l)) \\ &= \mathrm{Tr}\left[ (Z^{(\eta_l,\eta_l)}_{\checkmark} \otimes \mathbb{1}_E) U_{BE} \textstyle\sum_{i=0}^{d-1} \frac{\rho_{Z_i}(\mu_j)}{d} \otimes |0\rangle\langle 0|_E U^\dagger_{BE} \right], \end{aligned} \tag{D1}$$

where $Z^{(\eta_l,\eta_l)}_{\checkmark}$ is defined in Eq. (C171) and $\rho_{Z_i}(\mu_j)$ is given in Eq. (3). By using Eqs. (3) and (5), we can recast the gain as follows:

$$\begin{aligned} G^Z_{\mu_j,(\eta_l,\eta_l)} &= \sum_{n=0}^{\infty} e^{-\mu_j} \frac{\mu_j^n}{n!} \mathrm{Tr}\left[ (Z^{(\eta_l,\eta_l)}_{\checkmark} \otimes \mathbb{1}_E) U_{BE} \textstyle\sum_{i=0}^{d-1} \frac{|n_{Z_i}\rangle\langle n_{Z_i}|}{d} \otimes |0\rangle\langle 0|_E U^\dagger_{BE} \right] \\ &= \sum_{n=0}^{\infty} e^{-\mu_j} \frac{\mu_j^n}{n!} Y^Z_{n,(\eta_l,\eta_l)}, \end{aligned} \tag{D2}$$

where in the last equality we defined the $n$-photon $Z$-basis yield ($Y^Z_{n,(\eta_l,\eta_l)}$), by generalizing Eq. (C172).

Similarly, the $X$-basis gain in Eq. (12) is defined as the probability that Bob has a detection in the $X$-basis detector and in the $Z$-basis detector, given that Alice sent a state of the $X$-basis with intensity $\mu_j$ and Bob selected the TBS setting $(\eta_i, \eta_l)$. It can be expressed as

$$\begin{aligned} G^{X,\checkmark}_{\mu_j,(\eta_i,\eta_l)} &= \Pr(X_B \neq \emptyset, Z_B \neq \emptyset | T = X, I_A = \mu_j, (\eta_i, \eta_l)) \\ &= \mathrm{Tr}\left[ (X^{(\eta_i,\eta_l)}_{\checkmark,\checkmark} \otimes \mathbb{1}_E) U_{BE} \textstyle\sum_{k=0}^{d-1} \dfrac{\rho_{X_k}(\mu_j)}{d} \otimes |0\rangle\langle 0|_E U^\dagger_{BE} \right], \end{aligned} \tag{D3}$$

where $X^{(\eta_i,\eta_l)}_{\checkmark,\checkmark}$ is defined in Eq. (C272) and $\rho_{X_k}(\mu_j)$ is given in Eq. (6). By using Eq. (6), we can express the gain in terms of the $X$-basis yields:

$$G^{X,\checkmark}_{\mu_j,(\eta_i,\eta_l)} = \sum_{n=0}^{\infty} e^{-\mu_j} \frac{\mu_j^n}{n!} Y^{X,\checkmark}_{n,(\eta_i,\eta_l)}, \tag{D4}$$

where we defined the $n$-photon $X$-basis yields ($Y^{X,\checkmark}_{n,(\eta_i,\eta_l)}$) as a generalization of Eq. (C270). Analogously, we express the gain in Eq. (13) as follows:

$$G^{X,\emptyset}_{\mu_j,(\eta_i,\eta_l)} = \sum_{n=0}^{\infty} e^{-\mu_j} \frac{\mu_j^n}{n!} Y^{X,\emptyset}_{n,(\eta_i,\eta_l)}, \tag{D5}$$

where $Y^{X,\emptyset}_{n,(\eta_i,\eta_l)}$ generalizes Eq. (C271) to $n$ photons.

On the same lines, one can relate the $n$-photon $X$-basis bit error rates to the corresponding observed QBERs. In particular, the QBER in Eq. (15) is the probability that Bob's $X$-basis outcome differs from Alice's $X$-basis symbol, given that Bob had a detection in both detectors, Alice chose intensity $\mu_j$, and Bob chose the TBS setting $(\eta_i, \eta_\uparrow)$. Then, the product of this QBER and the corresponding $X$-basis gain reads

$$\begin{aligned} Q_{X,\mu_j,(\eta_i,\eta_\uparrow),\checkmark} G^{X,\checkmark}_{\mu_j,(\eta_i,\eta_\uparrow)} &= \Pr(X_B \neq \emptyset, Z_B \neq \emptyset, X_A \neq X_B | T = X, I_A = \mu_j, (\eta_i, \eta_\uparrow)) \\ &= \textstyle\sum_{k=0}^{d-1} \sum_{k' \neq k} \mathrm{Tr}\left[ (X^{(\eta_i,\eta_\uparrow)}_{k',\checkmark} \otimes \mathbb{1}_E) U_{BE} \dfrac{\rho_{X_k}(\mu_j)}{d} \otimes |0\rangle\langle 0|_E U^\dagger_{BE} \right], \end{aligned} \tag{D6}$$

where $X^{(\eta_i,\eta_\uparrow)}_{k',\checkmark}$ is defined in Eq. (C250). By using Eq. (6), we can expand the last expression in terms of the products of the $X$-basis yields and bit error rates as follows:

$$Q_{X,\mu_j,(\eta_i,\eta_\uparrow),\checkmark} G^{X,\checkmark}_{\mu_j,(\eta_i,\eta_\uparrow)} = \sum_{n=0}^{\infty} e^{-\mu_j} \frac{\mu_j^n}{n!} Y^{X,\checkmark}_{n,(\eta_i,\eta_\uparrow)} e_{X,n,(\eta_i,\eta_\uparrow),\checkmark}, \tag{D7}$$

where we defined the $n$-photon $X$-basis bit error rate ($e_{X,n,(\eta_i,\eta_\uparrow),\checkmark}$) as a generalization of Eq. (C274). Analogously, we have

$$Q_{X,\mu_j,(\eta_i,\eta_\uparrow),\emptyset} G^{X,\emptyset}_{\mu_j,(\eta_i,\eta_\uparrow)} = \sum_{n=0}^{\infty} e^{-\mu_j} \frac{\mu_j^n}{n!} Y^{X,\emptyset}_{n,(\eta_i,\eta_\uparrow)} e_{X,n,(\eta_i,\eta_\uparrow),\emptyset}, \tag{D8}$$

where $e_{X,n,(\eta_i,\eta_\uparrow),\emptyset}$ generalizes Eq. (C275).

### 2. Bounds on yields and bit error rates

We observe that the equations defining the decoy-state method, namely, Eqs. (D2), (D4), (D5), (D7), and (D8), share the same structure, which can be exemplified as follows:

$$G_{\mu_j} = \sum_{n=0}^{\infty} e^{-\mu_j} \frac{\mu_j^n}{n!} Y_n, \tag{D9}$$

where $G_{\mu_j}$ can be replaced by a gain or a product of QBER and gain, while $Y_n$ can be replaced by a yield or a product of yield and bit error rate. Then, starting from Eq. (D9) and following the procedure in the seminal paper on the decoy-state

method [39], one obtains the following lower bounds on the vacuum and one-photon yields:

$$\underline{Y_0} = \max\left\{0, \frac{\mu_2 e^{\mu_3} G_{\mu_3} - \mu_3 e^{\mu_2} G_{\mu_2}}{\mu_2 - \mu_3}\right\}, \tag{D10}$$

$$\underline{Y_1} = \max\left\{0, \frac{e^{\mu_2} G_{\mu_2} - e^{\mu_3} G_{\mu_3} - \frac{\mu_2^2 - \mu_3^2}{\mu_1^2}(e^{\mu_1} G_{\mu_1} - \underline{Y_0})}{(\mu_2 - \mu_3)\left(1 - \frac{\mu_2 + \mu_3}{\mu_1}\right)}\right\}. \tag{D11}$$

With similar techniques, one can derive a simple upper bound on the one-photon yield. To derive it, consider the following combination of gains in Eq. (D9):

$$e^{\mu_2} G_{\mu_2} - e^{\mu_3} G_{\mu_3} = (\mu_2 - \mu_3) Y_1 + \sum_{n=2}^{\infty} \frac{\mu_2^n - \mu_3^n}{n!} Y_n. \tag{D12}$$

Now observe that the sum on the right-hand side is composed only of non-negative terms since $\mu_2 > \mu_3$. Therefore, we can obtain the inequality

$$e^{\mu_2} G_{\mu_2} - e^{\mu_3} G_{\mu_3} \geq (\mu_2 - \mu_3) Y_1, \tag{D13}$$

which provides us with the upper bound on the one-photon yield:

$$Y_1 \leq \overline{Y_1} = \frac{e^{\mu_2} G_{\mu_2} - e^{\mu_3} G_{\mu_3}}{\mu_2 - \mu_3}. \tag{D14}$$

An alternative upper bound on $Y_1$ can be obtained by our using the statistics from all the intensity choices of Alice. In particular, we use the following linear combination of three gains:

$$\begin{aligned}
&(\mu_2^2 - \mu_3^2) e^{\mu_1} G_{\mu_1} - (\mu_1^2 - \mu_3^2) e^{\mu_2} G_{\mu_2} + (\mu_1^2 - \mu_2^2) e^{\mu_3} G_{\mu_3} \\
&= \sum_{n=0}^{\infty} \left[(\mu_2^2 - \mu_3^2)\frac{\mu_1^n}{n!} - (\mu_1^2 - \mu_3^2)\frac{\mu_2^n}{n!} + (\mu_1^2 - \mu_2^2)\frac{\mu_3^n}{n!}\right] Y_n \\
&= f(1) Y_1 + \sum_{n=3}^{\infty} f(n) Y_n,
\end{aligned} \tag{D15}$$

where we introduced

$$f(n) := (\mu_2^2 - \mu_3^2)\frac{\mu_1^n}{n!} - (\mu_1^2 - \mu_3^2)\frac{\mu_2^n}{n!} + (\mu_1^2 - \mu_2^2)\frac{\mu_3^n}{n!}. \tag{D16}$$

Now we observe that $f(1)$ is negative:

$$\begin{aligned}
& f(1) < 0 \\
\Leftrightarrow\ & (\mu_2^2 - \mu_3^2)\mu_1 - (\mu_1^2 - \mu_3^2)\mu_2 + (\mu_1^2 - \mu_2^2)\mu_3 < 0 \\
\Leftrightarrow\ & (\mu_2^2 - \mu_3^2)\mu_1 - (\mu_1^2 - \mu_2^2)\mu_2 - (\mu_2^2 - \mu_3^2)\mu_2 + (\mu_1^2 - \mu_2^2)\mu_3 < 0 \\
\Leftrightarrow\ & (\mu_2^2 - \mu_3^2)(\mu_1 - \mu_2) - (\mu_1^2 - \mu_2^2)(\mu_2 - \mu_3) < 0 \\
\Leftrightarrow\ & (\mu_2 - \mu_3)(\mu_1 - \mu_2)[\mu_2 + \mu_3 - \mu_1 - \mu_2] < 0,
\end{aligned} \tag{D17}$$

which is true since $\mu_3 < \mu_2 < \mu_1$. At the same time, we can show that $f(n) \geq 0$ for $n \geq 3$, as follows:

$$
\begin{aligned}
& f(n) \geq 0 \\
\Leftrightarrow \quad & (\mu_2^2-\mu_3^2)\mu_1^2\mu_1^{n-2} - (\mu_1^2-\mu_3^2)\mu_2^2\mu_2^{n-2} + (\mu_1^2-\mu_2^2)\mu_3^2\mu_3^{n-2} \geq 0 \\
\Leftrightarrow \quad & \mu_1^2\mu_2^2(\mu_1^{n-2}-\mu_2^{n-2}) - \mu_1^2\mu_3^2(\mu_1^{n-2}-\mu_3^{n-2}) + \mu_2^2\mu_3^2(\mu_2^{n-2}-\mu_3^{n-2}) \geq 0 \\
\Leftrightarrow \quad & \mu_1^2\mu_2^2(\mu_1^{n-2}-\mu_2^{n-2}) - \mu_1^2\mu_3^2(\mu_1^{n-2}-\mu_3^{n-2}) + \mu_2^2\mu_3^2\left[(\mu_1^{n-2}-\mu_3^{n-2}) - (\mu_1^{n-2}-\mu_2^{n-2})\right] \geq 0 \\
\Leftrightarrow \quad & \mu_2^2(\mu_1^{n-2}-\mu_2^{n-2})(\mu_1^2-\mu_3^2) - \mu_3^2(\mu_1^{n-2}-\mu_3^{n-2})(\mu_1^2-\mu_2^2) \geq 0 \\
\Leftrightarrow \quad & (\mu_1-\mu_2)(\mu_1-\mu_3) \\
& \left[\mu_2^2(\mu_1+\mu_3)(\mu_1^{n-3}+\mu_1^{n-4}\mu_2+\cdots+\mu_2^{n-3}) - \mu_3^2(\mu_1+\mu_2)(\mu_1^{n-3}+\mu_1^{n-4}\mu_3+\cdots+\mu_3^{n-3})\right] \geq 0 \\
\Leftrightarrow \quad & \mu_1\left[\mu_2^2(\mu_1^{n-3}+\mu_1^{n-4}\mu_2+\cdots+\mu_2^{n-3}) - \mu_3^2(\mu_1^{n-3}+\mu_1^{n-4}\mu_3+\cdots+\mu_3^{n-3})\right] \\
& + \mu_2\mu_3\left[\mu_2(\mu_1^{n-3}+\mu_1^{n-4}\mu_2+\cdots+\mu_2^{n-3}) - \mu_3(\mu_1^{n-3}+\mu_1^{n-4}\mu_3+\cdots+\mu_3^{n-3})\right] \geq 0,
\end{aligned}
\tag{D18}
$$

which is verified since $\mu_3 < \mu_2 < \mu_1$. Then we can derive an upper bound on $Y_1$ by replacing $Y_n$ with 1 in Eq. (D15), which yields

$$
(\mu_2^2-\mu_3^2)e^{\mu_1}G_{\mu_1} - (\mu_1^2-\mu_3^2)e^{\mu_2}G_{\mu_2} + (\mu_1^2-\mu_2^2)e^{\mu_3}G_{\mu_3} \leq f(1)Y_1 + \sum_{n=3}^{\infty} f(n), \tag{D19}
$$

where we can simplify the sum running over $n$ as follows:

$$
\begin{aligned}
\sum_{n=3}^{\infty} f(n) &= (\mu_2^2-\mu_3^2)\left(e^{\mu_1} - 1 - \mu_1 - \frac{\mu_1^2}{2}\right) \\
&\quad - (\mu_1^2-\mu_3^2)\left(e^{\mu_2} - 1 - \mu_2 - \frac{\mu_2^2}{2}\right) + (\mu_1^2-\mu_2^2)\left(e^{\mu_3} - 1 - \mu_3 - \frac{\mu_3^2}{2}\right) \\
&= (\mu_2^2-\mu_3^2)(e^{\mu_1}-\mu_1) - (\mu_1^2-\mu_3^2)(e^{\mu_2}-\mu_2) + (\mu_1^2-\mu_2^2)(e^{\mu_3}-\mu_3) \\
&= -f(1) + (\mu_2^2-\mu_3^2)e^{\mu_1} - (\mu_1^2-\mu_3^2)e^{\mu_2} + (\mu_1^2-\mu_2^2)e^{\mu_3}.
\end{aligned}
\tag{D20}
$$

By using the last expression in Eq. (D19), we obtain the following upper bound on the one-photon yield:

$$
\overline{Y_1} = 1 - \frac{(\mu_2^2-\mu_3^2)e^{\mu_1}(1-G_{\mu_1}) - (\mu_1^2-\mu_3^2)e^{\mu_2}(1-G_{\mu_2}) + (\mu_1^2-\mu_2^2)e^{\mu_3}(1-G_{\mu_3})}{(\mu_2^2-\mu_3^2)\mu_1 - (\mu_1^2-\mu_3^2)\mu_2 + (\mu_1^2-\mu_2^2)\mu_3}. \tag{D21}
$$

By combining Eqs. (D14) and (D21), we come to the final upper bound on the one-photon yield:

$$
\overline{Y_1} = \min\left\{1, \frac{e^{\mu_2}G_{\mu_2} - e^{\mu_3}G_{\mu_3}}{\mu_2-\mu_3}, 1 - \frac{(\mu_2^2-\mu_3^2)e^{\mu_1}(1-G_{\mu_1}) - (\mu_1^2-\mu_3^2)e^{\mu_2}(1-G_{\mu_2}) + (\mu_1^2-\mu_2^2)e^{\mu_3}(1-G_{\mu_3})}{(\mu_2^2-\mu_3^2)\mu_1 - (\mu_1^2-\mu_3^2)\mu_2 + (\mu_1^2-\mu_2^2)\mu_3}\right\}. \tag{D22}
$$

We can now substitute the appropriate yields and bit error rates in the generic bounds in Eqs. (D10), (D11), and (D22) to derive the required bounds appearing in the phase error rate upper bound (C437) and in the key rate expression (C56). For instance, by using the bound (D10) on the relations (D2), (D4), (D5), (D7), and (D8), we obtain, respectively,

$$
\underline{Y^Z_{0,(\eta_l,\eta_l)}} = \max\left\{0, \frac{\mu_2 e^{\mu_3}G^Z_{\mu_3,(\eta_l,\eta_l)} - \mu_3 e^{\mu_2}G^Z_{\mu_2,(\eta_l,\eta_l)}}{\mu_2-\mu_3}\right\}, \tag{D23}
$$

$$
\underline{Y^{X,\checkmark}_{0,(\eta_i,\eta_l)}} = \max\left\{0, \frac{\mu_2 e^{\mu_3}G^{X,\checkmark}_{\mu_3,(\eta_i,\eta_l)} - \mu_3 e^{\mu_2}G^{X,\checkmark}_{\mu_2,(\eta_i,\eta_l)}}{\mu_2-\mu_3}\right\}, \tag{D24}
$$

$$\underline{Y^{X,\emptyset}_{0,(\eta_i,\eta_l)}} = \max\left\{0, \frac{\mu_2 e^{\mu_3} G^{X,\emptyset}_{\mu_3,(\eta_i,\eta_l)} - \mu_3 e^{\mu_2} G^{X,\emptyset}_{\mu_2,(\eta_i,\eta_l)}}{\mu_2-\mu_3}\right\}, \tag{D25}$$

$$\underline{Y^{X,\checkmark}_{0,(\eta_i,\eta_\uparrow)} e_{X,0,(\eta_i,\eta_\uparrow),\checkmark}} = \max\left\{0, \frac{\mu_2 e^{\mu_3} Q_{X,\mu_3,(\eta_i,\eta_\uparrow),\checkmark} G^{X,\checkmark}_{\mu_3,(\eta_i,\eta_\uparrow)} - \mu_3 e^{\mu_2} Q_{X,\mu_2,(\eta_i,\eta_\uparrow),\checkmark} G^{X,\checkmark}_{\mu_2,(\eta_i,\eta_\uparrow)}}{\mu_2-\mu_3}\right\}, \tag{D26}$$

$$\underline{Y^{X,\emptyset}_{0,(\eta_i,\eta_\uparrow)} e_{X,0,(\eta_i,\eta_\uparrow),\emptyset}} = \max\left\{0, \frac{\mu_2 e^{\mu_3} Q_{X,\mu_3,(\eta_i,\eta_\uparrow),\emptyset} G^{X,\emptyset}_{\mu_3,(\eta_i,\eta_\uparrow)} - \mu_3 e^{\mu_2} Q_{X,\mu_2,(\eta_i,\eta_\uparrow),\emptyset} G^{X,\emptyset}_{\mu_2,(\eta_i,\eta_\uparrow)}}{\mu_2-\mu_3}\right\} \tag{D27}$$

for $\eta_i \in \{\eta_\uparrow, \eta_\downarrow, \eta_2\}$ and $\eta_l \in \{\eta_\downarrow, \eta_\uparrow\}$.

Similarly, we use the bound (D11) on and Eq. (D22) in Eq. (D2) to obtain

$$\underline{Y^{Z}_{1,(\eta_l,\eta_l)}} = \max\left\{0, \frac{e^{\mu_2} G^{Z}_{\mu_2,(\eta_l,\eta_l)} - e^{\mu_3} G^{Z}_{\mu_3,(\eta_l,\eta_l)} - \frac{\mu_2^2-\mu_3^2}{\mu_1^2}\left(e^{\mu_1} G^{Z}_{\mu_1,(\eta_l,\eta_l)} - \underline{Y^{Z}_{0,(\eta_l,\eta_l)}}\right)}{(\mu_2-\mu_3)\left(1-\frac{\mu_2+\mu_3}{\mu_1}\right)}\right\}, \tag{D28}$$

$$\begin{aligned}\overline{Y^{Z}_{1,(\eta_l,\eta_l)}} = \min\Bigg\{1, &\frac{e^{\mu_2} G^{Z}_{\mu_2,(\eta_l,\eta_l)} - e^{\mu_3} G^{Z}_{\mu_3,(\eta_l,\eta_l)}}{\mu_2-\mu_3},\\ &1 - \frac{(\mu_2^2-\mu_3^2)e^{\mu_1}(1-G^{Z}_{\mu_1,(\eta_l,\eta_l)}) - (\mu_1^2-\mu_3^2)e^{\mu_2}(1-G^{Z}_{\mu_2,(\eta_l,\eta_l)}) + (\mu_1^2-\mu_2^2)e^{\mu_3}(1-G^{Z}_{\mu_3,(\eta_l,\eta_l)})}{(\mu_2^2-\mu_3^2)\mu_1 - (\mu_1^2-\mu_3^2)\mu_2 + (\mu_1^2-\mu_2^2)\mu_3}\Bigg\}\end{aligned} \tag{D29}$$

for $\eta_l \in \{\eta_\downarrow, \eta_\uparrow\}$.

Subsequently, we use the bounds (D11) and (D22) on Eqs. (D4) and (D5) to obtain

$$\underline{Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}} = \max\left\{0, \frac{e^{\mu_2} G^{X,\checkmark}_{\mu_2,(\eta_i,\eta_l)} - e^{\mu_3} G^{X,\checkmark}_{\mu_3,(\eta_i,\eta_l)} - \frac{\mu_2^2-\mu_3^2}{\mu_1^2}\left(e^{\mu_1} G^{X,\checkmark}_{\mu_1,(\eta_i,\eta_l)} - \underline{Y^{X,\checkmark}_{0,(\eta_i,\eta_l)}}\right)}{(\mu_2-\mu_3)\left(1-\frac{\mu_2+\mu_3}{\mu_1}\right)}\right\}, \tag{D30}$$

$$\underline{Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}} = \max\left\{0, \frac{e^{\mu_2} G^{X,\emptyset}_{\mu_2,(\eta_i,\eta_l)} - e^{\mu_3} G^{X,\emptyset}_{\mu_3,(\eta_i,\eta_l)} - \frac{\mu_2^2-\mu_3^2}{\mu_1^2}\left(e^{\mu_1} G^{X,\emptyset}_{\mu_1,(\eta_i,\eta_l)} - \underline{Y^{X,\emptyset}_{0,(\eta_i,\eta_l)}}\right)}{(\mu_2-\mu_3)\left(1-\frac{\mu_2+\mu_3}{\mu_1}\right)}\right\}, \tag{D31}$$

$$\begin{aligned}\overline{Y^{X,\checkmark}_{1,(\eta_i,\eta_l)}} = \min\Bigg\{1, &\frac{e^{\mu_2} G^{X,\checkmark}_{\mu_2,(\eta_i,\eta_l)} - e^{\mu_3} G^{X,\checkmark}_{\mu_3,(\eta_i,\eta_l)}}{\mu_2-\mu_3},\\ &1 - \frac{(\mu_2^2-\mu_3^2)e^{\mu_1}(1-G^{X,\checkmark}_{\mu_1,(\eta_i,\eta_l)}) - (\mu_1^2-\mu_3^2)e^{\mu_2}(1-G^{X,\checkmark}_{\mu_2,(\eta_i,\eta_l)}) + (\mu_1^2-\mu_2^2)e^{\mu_3}(1-G^{X,\checkmark}_{\mu_3,(\eta_i,\eta_l)})}{(\mu_2^2-\mu_3^2)\mu_1 - (\mu_1^2-\mu_3^2)\mu_2 + (\mu_1^2-\mu_2^2)\mu_3}\Bigg\},\end{aligned} \tag{D32}$$

$$\begin{aligned}\overline{Y^{X,\emptyset}_{1,(\eta_i,\eta_l)}} = \min\Bigg\{1, &\frac{e^{\mu_2} G^{X,\emptyset}_{\mu_2,(\eta_i,\eta_l)} - e^{\mu_3} G^{X,\emptyset}_{\mu_3,(\eta_i,\eta_l)}}{\mu_2-\mu_3},\\ &1 - \frac{(\mu_2^2-\mu_3^2)e^{\mu_1}(1-G^{X,\emptyset}_{\mu_1,(\eta_i,\eta_l)}) - (\mu_1^2-\mu_3^2)e^{\mu_2}(1-G^{X,\emptyset}_{\mu_2,(\eta_i,\eta_l)}) + (\mu_1^2-\mu_2^2)e^{\mu_3}(1-G^{X,\emptyset}_{\mu_3,(\eta_i,\eta_l)})}{(\mu_2^2-\mu_3^2)\mu_1 - (\mu_1^2-\mu_3^2)\mu_2 + (\mu_1^2-\mu_2^2)\mu_3}\Bigg\}\end{aligned} \tag{D33}$$

for $\eta_i \in \{\eta_\uparrow, \eta_\downarrow, \eta_2\}$ and $\eta_l \in \{\eta_\downarrow, \eta_\uparrow\}$.

Finally, we use the bounds (D11) and (D22) on Eqs. (D7) and (D8) to obtain

$$\underline{Y^{X,\checkmark}_{1,(\eta_i,\eta_\uparrow)} e_{X,1,(\eta_i,\eta_\uparrow),\checkmark}} = \max\left\{0, \frac{e^{\mu_2} Q_{X,\mu_2,(\eta_i,\eta_\uparrow),\checkmark} G^{X,\checkmark}_{\mu_2,(\eta_i,\eta_\uparrow)} - e^{\mu_3} Q_{X,\mu_3,(\eta_i,\eta_\uparrow),\checkmark} G^{X,\checkmark}_{\mu_3,(\eta_i,\eta_\uparrow)}}{(\mu_2-\mu_3)\left(1-\frac{\mu_2+\mu_3}{\mu_1}\right)} - \frac{\frac{\mu_2^2-\mu_3^2}{\mu_1^2}\left(e^{\mu_1} Q_{X,\mu_1,(\eta_i,\eta_\uparrow),\checkmark} G^{X,\checkmark}_{\mu_1,(\eta_i,\eta_\uparrow)} - \underline{Y^{X,\checkmark}_{0,(\eta_i,\eta_\uparrow)} e_{X,0,(\eta_i,\eta_\uparrow),\checkmark}}\right)}{(\mu_2-\mu_3)\left(1-\frac{\mu_2+\mu_3}{\mu_1}\right)}\right\}, \tag{D34}$$

$$\underline{Y^{X,\emptyset}_{1,(\eta_i,\eta_\uparrow)} e_{X,1,(\eta_i,\eta_\uparrow),\emptyset}} = \max\left\{0, \frac{e^{\mu_2} Q_{X,\mu_2,(\eta_i,\eta_\uparrow),\emptyset} G^{X,\emptyset}_{\mu_2,(\eta_i,\eta_\uparrow)} - e^{\mu_3} Q_{X,\mu_3,(\eta_i,\eta_\uparrow),\emptyset} G^{X,\emptyset}_{\mu_3,(\eta_i,\eta_\uparrow)}}{(\mu_2-\mu_3)\left(1-\frac{\mu_2+\mu_3}{\mu_1}\right)} - \frac{\frac{\mu_2^2-\mu_3^2}{\mu_1^2}\left(e^{\mu_1} Q_{X,\mu_1,(\eta_i,\eta_\uparrow),\emptyset} G^{X,\emptyset}_{\mu_1,(\eta_i,\eta_\uparrow)} - \underline{Y^{X,\emptyset}_{0,(\eta_i,\eta_\uparrow)} e_{X,0,(\eta_i,\eta_\uparrow),\emptyset}}\right)}{(\mu_2-\mu_3)\left(1-\frac{\mu_2+\mu_3}{\mu_1}\right)}\right\}, \tag{D35}$$

$$\begin{aligned}\overline{Y^{X,\checkmark}_{1,(\eta_i,\eta_\uparrow)} e_{X,1,(\eta_i,\eta_\uparrow),\checkmark}} = \min\Bigg\{1, &\frac{e^{\mu_2} Q_{X,\mu_2,(\eta_i,\eta_\uparrow),\checkmark} G^{X,\checkmark}_{\mu_2,(\eta_i,\eta_\uparrow)} - e^{\mu_3} Q_{X,\mu_3,(\eta_i,\eta_\uparrow),\checkmark} G^{X,\checkmark}_{\mu_3,(\eta_i,\eta_\uparrow)}}{\mu_2-\mu_3},\\ &1-\Bigg(\frac{(\mu_2^2-\mu_3^2)e^{\mu_1}(1-Q_{X,\mu_1,(\eta_i,\eta_\uparrow),\checkmark} G^{X,\checkmark}_{\mu_1,(\eta_i,\eta_\uparrow)}) - (\mu_1^2-\mu_3^2)e^{\mu_2}(1-Q_{X,\mu_2,(\eta_i,\eta_\uparrow),\checkmark} G^{X,\checkmark}_{\mu_2,(\eta_i,\eta_\uparrow)})}{(\mu_2^2-\mu_3^2)\mu_1-(\mu_1^2-\mu_3^2)\mu_2+(\mu_1^2-\mu_2^2)\mu_3}\\ &+\frac{(\mu_1^2-\mu_2^2)e^{\mu_3}(1-Q_{X,\mu_3,(\eta_i,\eta_\uparrow),\checkmark} G^{X,\checkmark}_{\mu_3,(\eta_i,\eta_\uparrow)})}{(\mu_2^2-\mu_3^2)\mu_1-(\mu_1^2-\mu_3^2)\mu_2+(\mu_1^2-\mu_2^2)\mu_3}\Bigg)\Bigg\},\end{aligned} \tag{D36}$$

and

$$\begin{aligned}\overline{Y^{X,\emptyset}_{1,(\eta_i,\eta_\uparrow)} e_{X,1,(\eta_i,\eta_\uparrow),\emptyset}} = \min\Bigg\{1, &\frac{e^{\mu_2} Q_{X,\mu_2,(\eta_i,\eta_\uparrow),\emptyset} G^{X,\emptyset}_{\mu_2,(\eta_i,\eta_\uparrow)} - e^{\mu_3} Q_{X,\mu_3,(\eta_i,\eta_\uparrow),\emptyset} G^{X,\emptyset}_{\mu_3,(\eta_i,\eta_\uparrow)}}{\mu_2-\mu_3},\\ &1-\Bigg(\frac{(\mu_2^2-\mu_3^2)e^{\mu_1}(1-Q_{X,\mu_1,(\eta_i,\eta_\uparrow),\emptyset} G^{X,\emptyset}_{\mu_1,(\eta_i,\eta_\uparrow)}) - (\mu_1^2-\mu_3^2)e^{\mu_2}(1-Q_{X,\mu_2,(\eta_i,\eta_\uparrow),\emptyset} G^{X,\emptyset}_{\mu_2,(\eta_i,\eta_\uparrow)})}{(\mu_2^2-\mu_3^2)\mu_1-(\mu_1^2-\mu_3^2)\mu_2+(\mu_1^2-\mu_2^2)\mu_3}\\ &+\frac{(\mu_1^2-\mu_2^2)e^{\mu_3}(1-Q_{X,\mu_3,(\eta_i,\eta_\uparrow),\emptyset} G^{X,\emptyset}_{\mu_3,(\eta_i,\eta_\uparrow)})}{(\mu_2^2-\mu_3^2)\mu_1-(\mu_1^2-\mu_3^2)\mu_2+(\mu_1^2-\mu_2^2)\mu_3}\Bigg)\Bigg\}\end{aligned} \tag{D37}$$

for $\eta_i \in \{\eta_\uparrow, \eta_\downarrow, \eta_2\}$.

### 3. Bounds on linear combinations of yields

Some of the quantities appearing in the phase error rate bound (B1), namely, Eqs. (B5)–(B9), depend on linear combinations of one-photon $Z$-basis yields. In principle, in these expressions we could use the bounds already derived for the single yields. However, to obtain a tighter bound, in the following we derive bounds on the whole linear combination of the yields.

To start with, we observe that the linear combinations of yields in Eqs. (B6)–(B9) can be generically written in the form

$$c_\uparrow Y^Z_{1,(\eta_\uparrow,\eta_\uparrow)} - c_\downarrow Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}, \tag{D38}$$

where the coefficients $c_\uparrow$ and $c_\downarrow$ depend on the particular linear combination that is considered. Then we can obtain a tighter upper bound on Eq. (D38) by considering the following equation:

$$\tilde{G}^Z_{\mu_j} = \sum_{n=0}^{\infty} e^{-\mu_j} \frac{\mu_j^n}{n!} \tilde{Y}^Z_n, \tag{D39}$$

where we defined

$$\tilde{G}^Z_{\mu_j} := c_\uparrow G^Z_{\mu_j,(\eta_\uparrow,\eta_\uparrow)} - c_\downarrow G^Z_{\mu_j,(\eta_\downarrow,\eta_\downarrow)}, \tag{D40}$$

$$\tilde{Y}^Z_n := c_\uparrow Y^Z_{n,(\eta_\uparrow,\eta_\uparrow)} - c_\downarrow Y^Z_{n,(\eta_\downarrow,\eta_\downarrow)}. \tag{D41}$$

We observe that Eq. (D39) has the same form as the standard equation of the decoy-state method, Eq. (D9), with the important difference that the new gains ($\tilde{G}^Z_{\mu_j}$) and new yields ($\tilde{Y}^Z_n$) are not necessarily non-negative. In other words, while $0 \leq Y_n \leq 1$ for every yield, this is not true anymore for $\tilde{Y}^Z_n$. Nevertheless, we can still apply the techniques of the standard decoy-state method to Eq. (D39), as far as we can obtain an interval of existence for the new yields $\tilde{Y}^Z_n$.

To this aim, we recall from Eq. (D2) that the $n$-photon $Z$-basis yield can be written as

$$Y^Z_{n,(\eta_l,\eta_l)} = \mathrm{Tr}\left[\sigma_n Z^{(\eta_l,\eta_l)}_{\checkmark}\right], \tag{D42}$$

with

$$\sigma_n := \mathrm{Tr}_E\left[U_{BE} \textstyle\sum_{i=0}^{d-1} \frac{|n_{Z_i}\rangle\langle n_{Z_i}|}{d} \otimes |0\rangle\langle 0|_E U^\dagger_{BE}\right]. \tag{D43}$$

By using Eq. (C179) for $Z^{(\eta_l,\eta_l)}_{\checkmark}$ in Eq. (D42), we can express the new yield (D41) as follows:

$$\tilde{Y}^Z_n = \sum_{\alpha=0}^{\infty} \mathrm{Tr}\left[\sigma_n \Pi^\alpha_{\mathcal{Z}}\right] \left\{c_\uparrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\uparrow^\alpha\right] - c_\downarrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\downarrow^\alpha\right]\right\}. \tag{D44}$$

From the last expression, we can immediately derive an interval of existence for $\tilde{Y}^Z_n$:

$$\underline{\tilde{Y}^Z} \leq \tilde{Y}^Z_n \leq \overline{\tilde{Y}^Z}, \tag{D45}$$

where we defined

$$\underline{\tilde{Y}^Z} = \min_{\alpha\geq 0}\left\{c_\uparrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\uparrow^\alpha\right] - c_\downarrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\downarrow^\alpha\right]\right\}, \tag{D46}$$

$$\overline{\tilde{Y}^Z} = \max_{\alpha\geq 0}\left\{c_\uparrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\uparrow^\alpha\right] - c_\downarrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\downarrow^\alpha\right]\right\}. \tag{D47}$$

Clearly, the interval of existence of $\tilde{Y}^Z_n$ is independent of $n$ (as for the standard yields) but depends on the particular linear combination of yields, i.e., on $c_\uparrow$ and $c_\downarrow$. It is useful to derive a necessary and sufficient condition for the terms in Eqs. (D46) and (D47) to be increasing with $\alpha$,

$$\begin{aligned} & c_\uparrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\uparrow^\alpha\right] - c_\downarrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\downarrow^\alpha\right] \leq c_\uparrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\uparrow^{\alpha+1}\right] - c_\downarrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\downarrow^{\alpha+1}\right] \\ \iff\quad & c_\downarrow\eta_\downarrow^\alpha - c_\uparrow\eta_\uparrow^\alpha \leq c_\downarrow\eta_\downarrow^{\alpha+1} - c_\uparrow\eta_\uparrow^{\alpha+1} \\ \iff\quad & c_\downarrow(1-\eta_\downarrow)\eta_\downarrow^\alpha \leq c_\uparrow(1-\eta_\uparrow)\eta_\uparrow^\alpha, \end{aligned} \tag{D48}$$

which can then be applied to the specific cases of $c_\uparrow$ and $c_\downarrow$.

We can now derive an upper bound on Eq. (D38) by following the same procedure that leads to Eq. (D14). In particular, we consider the following combination of new gains in Eq. (D39):

$$\begin{aligned} e^{\mu_2}\tilde{G}^Z_{\mu_2} - e^{\mu_3}\tilde{G}^Z_{\mu_3} &= (\mu_2-\mu_3)\tilde{Y}^Z_1 + \sum_{n=2}^{\infty}\frac{\mu_2^n-\mu_3^n}{n!}\tilde{Y}^Z_n \\ &\geq (\mu_2-\mu_3)\tilde{Y}^Z_1 + \underline{\tilde{Y}^Z}\sum_{n=2}^{\infty}\frac{\mu_2^n-\mu_3^n}{n!} \\ &= (\mu_2-\mu_3)\tilde{Y}^Z_1 + \underline{\tilde{Y}^Z}\,(e^{\mu_2}-e^{\mu_3}+\mu_3-\mu_2)\,. \end{aligned} \tag{D49}$$

This leads to the following upper bound on $\tilde{Y}^Z_1$:

$$\tilde{Y}^Z_1 = c_\uparrow Y^Z_{1,(\eta_\uparrow,\eta_\uparrow)} - c_\downarrow Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)} \leq \overline{c_\uparrow Y^Z_{1,(\eta_\uparrow,\eta_\uparrow)} - c_\downarrow Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}, \tag{D50}$$

with

$$\begin{aligned} \overline{c_\uparrow Y^Z_{1,(\eta_\uparrow,\eta_\uparrow)} - c_\downarrow Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}} := \min\Bigg\{ &\overline{\tilde{Y}^Z}, \frac{c_\uparrow(e^{\mu_2}G^Z_{\mu_2,(\eta_\uparrow,\eta_\uparrow)} - e^{\mu_3}G^Z_{\mu_3,(\eta_\uparrow,\eta_\uparrow)}) - c_\downarrow(e^{\mu_2}G^Z_{\mu_2,(\eta_\downarrow,\eta_\downarrow)} - e^{\mu_3}G^Z_{\mu_3,(\eta_\downarrow,\eta_\downarrow)})}{\mu_2-\mu_3} \\ &-\frac{\underline{\tilde{Y}^Z}\,(e^{\mu_2}-e^{\mu_3}+\mu_3-\mu_2)}{\mu_2-\mu_3}\Bigg\}. \end{aligned} \tag{D51}$$

This upper bound can be applied to each expression in Eqs. (B6)–(B9) by one replacing $c_\uparrow$ and $c_\downarrow$ with the appropriate coefficients from Eq. (B5)–(B9) and by using the explicit expressions for $\underline{\tilde{Y}^Z}$ and $\overline{\tilde{Y}^Z}$. The latter are obtained from Eqs. (D46) and (D47) for specific choices of $c_\uparrow$ and $c_\downarrow$:

(1) For $c_\uparrow = \eta_\downarrow$ and $c_\downarrow = \eta_\uparrow(1-\eta_\uparrow)$: In this case the condition in Eq. (D48) becomes $(1-\eta_\downarrow)\eta_\downarrow^{\alpha-1} \leq \eta_\uparrow^{\alpha-1}$, which is true if $\alpha \geq 1$. Moreover, since the inequality

$$\begin{aligned} &\left\{c_\uparrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\uparrow^\alpha\right] - c_\downarrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\downarrow^\alpha\right]\right\}_{\alpha=0} \geq \left\{c_\uparrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\uparrow^\alpha\right] - c_\downarrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\downarrow^\alpha\right]\right\}_{\alpha=1} \\ \iff \quad &\eta_\uparrow \geq \frac{\eta_\downarrow}{1-\eta_\downarrow} \end{aligned} \tag{D52}$$

is true due to Eq. (9), we have that Eqs. (D46) and (D47) are given by

$$\underline{\tilde{Y}^Z} = \left\{c_\uparrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\uparrow^\alpha\right] - c_\downarrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\downarrow^\alpha\right]\right\}_{\alpha=1} = \eta_\downarrow - \eta_\uparrow(1-\eta_\uparrow) - (1-p_d^{\mathcal{Z}})\eta_\downarrow\eta_\uparrow^2, \tag{D53}$$

$$\begin{aligned} \overline{\tilde{Y}^Z} &= \max\left[\left\{c_\uparrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\uparrow^\alpha\right] - c_\downarrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\downarrow^\alpha\right]\right\}_{\alpha=0}, \left\{c_\uparrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\uparrow^\alpha\right] - c_\downarrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\downarrow^\alpha\right]\right\}_{\alpha\to\infty}\right] \\ &= \max\left\{p_d^{\mathcal{Z}}\left[\eta_\downarrow - \eta_\uparrow(1-\eta_\uparrow)\right], \eta_\downarrow - \eta_\uparrow(1-\eta_\uparrow)\right\}. \end{aligned} \tag{D54}$$

(2) For $c_\uparrow = -\eta_\downarrow(1-\eta_\downarrow)$ and $c_\downarrow = -\eta_\uparrow$: In this case the condition in Eq. (D48) becomes $\eta_\downarrow^{\alpha-1} \geq (1-\eta_\uparrow)\eta_\uparrow^{\alpha-1}$, which is verified for $\alpha = 0, 1$ but it is not clear for what $\alpha$ it does not hold. To find good estimations of $\underline{\tilde{Y}^Z}$ and $\overline{\tilde{Y}^Z}$ in this case,

we define $f(\alpha)$ to be the argument of the optimizations in Eqs. (D46) and (D47),

$$f(\alpha) := \eta_\uparrow - \eta_\downarrow(1-\eta_\downarrow) + (1-p_d^{\mathcal{Z}})\eta_\uparrow\eta_\downarrow\left[(1-\eta_\downarrow)\eta_\uparrow^{\alpha-1} - \eta_\downarrow^{\alpha-1}\right], \tag{D55}$$

and find the condition for which its first derivative is non-negative: $f'(\alpha) \geq 0$. We obtain

$$\alpha \leq 1 + \frac{\ln\left[(1-\eta_\downarrow)^{\frac{\ln\eta_\uparrow}{\ln\eta_\downarrow}}\right]}{\ln\eta_\downarrow - \ln\eta_\uparrow}, \tag{D56}$$

which implies $\alpha < 1$. Thus, we conclude that $f(\alpha)$ is minimal at the two extremes of $\alpha$'s range—$f(0)$ and $f(\infty)$—and since $\eta_\uparrow > \eta_\downarrow(1-\eta_\downarrow)$, we get

$$\underline{\tilde{Y}^Z} = \left\{c_\uparrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\uparrow^\alpha\right] - c_\downarrow\left[1-(1-p_d^{\mathcal{Z}})\eta_\downarrow^\alpha\right]\right\}_{\alpha=0} = p_d^{\mathcal{Z}}\left[\eta_\uparrow - \eta_\downarrow(1-\eta_\downarrow)\right], \tag{D57}$$

$$\overline{\tilde{Y}^Z} = \eta_\uparrow, \tag{D58}$$

while for $\overline{\tilde{Y}^Z}$ we used the definition (D41) and the fact that $0 \leq Y_n^Z \leq 1$.

(3) For $c_\uparrow = -(1-\eta_\downarrow^2)$ and $c_\downarrow = -1$: In this case the condition in Eq. (D48) becomes $\eta_\downarrow^\alpha \geq (1+\eta_\downarrow)(1-\eta_\uparrow)\eta_\uparrow^\alpha$, which is verified for $\alpha = 0$. Similarly to before, we define $f(\alpha)$ to be the argument of the optimizations in Eqs. (D46) and (D47),

$$f(\alpha) := 1 - (1-\eta_\downarrow^2) + (1-p_d^{\mathcal{Z}})\left[(1-\eta_\downarrow^2)\eta_\uparrow^\alpha - \eta_\downarrow^\alpha\right], \tag{D59}$$

and find the condition for which its first derivative is non-negative: $f'(\alpha) \geq 0$. We obtain

$$\alpha \leq \frac{\ln\left[(1-\eta_\downarrow^2)^{\frac{\ln\eta_\uparrow}{\ln\eta_\downarrow}}\right]}{\ln\eta_\downarrow - \ln\eta_\uparrow}, \tag{D60}$$

which implies that $f(\alpha)$ stops increasing for a value $\alpha > 0$. Thus, $f(\alpha)$ has its global minimum in either $\alpha = 0$ or $\alpha = \infty$. We obtain

$$\underline{\tilde{Y}^Z} = p_d^{\mathcal{Z}}\left[1-(1-\eta_\downarrow^2)\right], \tag{D61}$$

$$\overline{\tilde{Y}^Z} = 1, \tag{D62}$$

where for $\overline{\tilde{Y}^Z}$ we again used the definition (D41) and the fact that $0 \leq Y_n^Z \leq 1$.

(4) For $c_\uparrow = 1$ and $c_\downarrow = 1-\eta_\uparrow^2$: In this case the condition in Eq. (D48) becomes $(1+\eta_\uparrow)(1-\eta_\downarrow)\eta_\downarrow^\alpha \leq \eta_\uparrow^\alpha$, which is not verified for $\alpha = 0$ due to Eq. (9). Therefore, given that $f(\alpha)$ is the argument of the optimizations in Eqs. (D46) and (D47),

$$f(\alpha) := 1 - (1-\eta_\uparrow^2) + (1-p_d^{\mathcal{Z}})\left[(1-\eta_\uparrow^2)\eta_\downarrow^\alpha - \eta_\uparrow^\alpha\right], \tag{D63}$$

we found that $f(0) > f(1)$. Now we find the condition for which its first derivative is negative: $f'(\alpha) < 0$. We obtain

$$\alpha < \frac{\ln\left[\frac{\ln\eta_\uparrow}{(1-\eta_\uparrow^2)\ln\eta_\downarrow}\right]}{\ln\eta_\downarrow - \ln\eta_\uparrow}, \tag{D64}$$

and since we know that $f(0) > f(1)$, it must be that $f(\alpha)$ stops decreasing at some point greater than zero. Then we conclude that $f(\alpha)$ is maximal at the extremes and we obtain

$$\underline{\tilde{Y}^Z} = -(1-\eta_\uparrow^2), \tag{D65}$$

$$\overline{\tilde{Y}^Z} = \eta_\uparrow^2, \tag{D66}$$

where for $\underline{\tilde{Y}^Z}$ we used the definition (D41) and the fact that $0 \leq Y_n^Z \leq 1$.

Finally, we derive an upper bound on the linear combination of yields that appears in Eq. (B5), namely,

$$(\eta_\uparrow - \eta_\downarrow) Y^Z_{1,(\eta_2,\eta_2)} - (1-\eta_2)(Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)} - Y^Z_{1,(\eta_\uparrow,\eta_\uparrow)}) - (\eta_\uparrow - \eta_\downarrow) p_d^{\mathcal{Z}}. \tag{D67}$$

This can again be done by our applying the decoy-state method on the formula in Eq. (D39), where this time we define the gain and the yield to be

$$\tilde{G}^Z_{\mu_j} := (\eta_\uparrow - \eta_\downarrow) G^Z_{\mu_j,(\eta_2,\eta_2)} - (1-\eta_2)\left(G^Z_{\mu_j,(\eta_\downarrow,\eta_\downarrow)} - G^Z_{\mu_j,(\eta_\uparrow,\eta_\uparrow)}\right) - (\eta_\uparrow - \eta_\downarrow) p_d^{\mathcal{Z}}, \tag{D68}$$

$$\tilde{Y}^Z_n := (\eta_\uparrow - \eta_\downarrow) Y^Z_{n,(\eta_2,\eta_2)} - (1-\eta_2)\left(Y^Z_{n,(\eta_\downarrow,\eta_\downarrow)} - Y^Z_{n,(\eta_\uparrow,\eta_\uparrow)}\right) - (\eta_\uparrow - \eta_\downarrow) p_d^{\mathcal{Z}}. \tag{D69}$$

Our goal is to derive an upper bound on $\tilde{Y}^Z_1$. Similarly to Eq. (D44), we can recast the newly defined yield in Eq. (D69) as follows:

$$\tilde{Y}^Z_n = \sum_{\alpha=0}^{\infty} \mathrm{Tr}\left[\sigma_n \Pi^\alpha_{\mathcal{Z}}\right] \gamma_\alpha, \tag{D70}$$

where we introduced

$$\gamma_\alpha := (1 - p_d^{\mathcal{Z}})\left[(\eta_\uparrow - \eta_\downarrow)(1-\eta_2^\alpha) - (1-\eta_2)(\eta_\uparrow^\alpha - \eta_\downarrow^\alpha)\right]. \tag{D71}$$

To derive an interval of existence for $\tilde{Y}^Z_n$, i.e., $\underline{\tilde{Y}^Z} \le \tilde{Y}^Z_n \le \overline{\tilde{Y}^Z}$, we notice that $\gamma_0 = \gamma_1 = 0$ and that $\gamma_\alpha \ge 0$ for every $\alpha \ge 2$ [this last result can be directly inferred from the study of $g(\alpha)$ in Eq. (C211)]. Then we have

$$\underline{\tilde{Y}^Z} = \gamma_0 = 0. \tag{D72}$$

For the upper bound, we observe that $\gamma_\alpha \le \gamma_{\alpha+1}$ for $\alpha \ge 2$. Indeed,

$$\begin{aligned}
& \gamma_\alpha \le \gamma_{\alpha+1} \\
\Leftrightarrow\ & (\eta_\uparrow - \eta_\downarrow)(-\eta_2^\alpha) - (1-\eta_2)(\eta_\uparrow^\alpha - \eta_\downarrow^\alpha) \le (\eta_\uparrow - \eta_\downarrow)(-\eta_2^{\alpha+1}) - (1-\eta_2)(\eta_\uparrow^{\alpha+1} - \eta_\downarrow^{\alpha+1}) \\
\Leftrightarrow\ & -(1-\eta_2)(\eta_\uparrow^\alpha - \eta_\downarrow^\alpha) \le (\eta_\uparrow - \eta_\downarrow)\eta_2^\alpha(1-\eta_2) - (1-\eta_2)(\eta_\uparrow^{\alpha+1} - \eta_\downarrow^{\alpha+1}) \\
\Leftrightarrow\ & 0 \le (\eta_\uparrow^\alpha - \eta_\downarrow^\alpha) + (\eta_\uparrow - \eta_\downarrow)\eta_2^\alpha - (\eta_\uparrow^{\alpha+1} - \eta_\downarrow^{\alpha+1}) \\
\Leftrightarrow\ & 0 \le (\eta_\uparrow - \eta_\downarrow)(\eta_2^\alpha + \eta_\uparrow^{\alpha-1} + \eta_\uparrow^{\alpha-2}\eta_\downarrow + \cdots + \eta_\uparrow\eta_\downarrow^{\alpha-2} + \eta_\downarrow^{\alpha-1}) \\
& \qquad - (\eta_\uparrow - \eta_\downarrow)(\eta_\uparrow^\alpha + \eta_\uparrow^{\alpha-1}\eta_\downarrow + \cdots + \eta_\uparrow\eta_\downarrow^{\alpha-1} + \eta_\downarrow^\alpha) \\
\Leftrightarrow\ & \eta_2^\alpha + \eta_\uparrow^{\alpha-1} + \eta_\uparrow^{\alpha-2}\eta_\downarrow + \cdots + \eta_\uparrow\eta_\downarrow^{\alpha-2} + \eta_\downarrow^{\alpha-1} \ge \eta_\uparrow^\alpha + \eta_\uparrow^{\alpha-1}\eta_\downarrow + \cdots + \eta_\uparrow\eta_\downarrow^{\alpha-1} + \eta_\downarrow^\alpha \\
\Leftrightarrow\ & \eta_\uparrow^{\alpha-1}(1-\eta_\uparrow) + \eta_\uparrow^{\alpha-2}\eta_\downarrow(1-\eta_\uparrow) + \cdots + \eta_\uparrow\eta_\downarrow^{\alpha-2}(1-\eta_\uparrow) + \eta_\downarrow^{\alpha-1}(1-\eta_\uparrow) + (\eta_2^\alpha - \eta_\downarrow^\alpha) \ge 0,
\end{aligned} \tag{D73}$$

which is true since $\eta_2 > \eta_\downarrow$ and $1 \ge \eta_\uparrow$. Then we have

$$\overline{\tilde{Y}^Z} = \gamma_\infty = (1 - p_d^{\mathcal{Z}})(\eta_\uparrow - \eta_\downarrow). \tag{D74}$$

We can now derive an upper bound on $\tilde{Y}^Z_1$ in the same way used to derive an upper bound on the one-photon yield with two or three decoy intensities, Eq. (D22). We start by obtaining the bound with two decoy intensities. Consider the decoy-state formula in Eq. (D39) and consider the combination of gains that leads to Eq. (D49). We obtain the following upper bound on $\tilde{Y}^Z_1$:

$$\tilde{Y}^Z_1 \le C(\mu_2, \mu_3), \tag{D75}$$

where we defined

$$C(\mu_2,\mu_3) := \frac{e^{\mu_2}\tilde{G}^Z_{\mu_2} - e^{\mu_3}\tilde{G}^Z_{\mu_3} - \underline{\tilde{Y}^Z}\,(e^{\mu_2} - e^{\mu_3} + \mu_3 - \mu_2)}{\mu_2 - \mu_3}. \tag{D76}$$

By substituting $\underline{\tilde{Y}^Z} = 0$ and $\tilde{G}_{\mu_j}$ with Eq. (D68) in the last expression, we obtain

$$\begin{aligned} C(\mu_2,\mu_3) = e^{\mu_2}&\frac{(\eta_\uparrow - \eta_\downarrow)\left(G^Z_{\mu_2,(\eta_2,\eta_2)} - p_d^{\mathcal{Z}}\right) - (1-\eta_2)\left(G^Z_{\mu_2,(\eta_\downarrow,\eta_\downarrow)} - G^Z_{\mu_2,(\eta_\uparrow,\eta_\uparrow)}\right)}{\mu_2 - \mu_3} \\ - e^{\mu_3}&\frac{(\eta_\uparrow - \eta_\downarrow)\left(G^Z_{\mu_3,(\eta_2,\eta_2)} - p_d^{\mathcal{Z}}\right) - (1-\eta_2)\left(G^Z_{\mu_3,(\eta_\downarrow,\eta_\downarrow)} - G^Z_{\mu_3,(\eta_\uparrow,\eta_\uparrow)}\right)}{\mu_2 - \mu_3}. \end{aligned} \tag{D77}$$

For the case of three decoy intensities, we consider the same combination of gains as in Eq. (D15). Then, in the resulting expression, we can replace $\tilde{Y}^Z_n$ with $\overline{\tilde{Y}^Z}$ (instead of 1) and follow the same steps leading to Eq. (D21). By doing so, we obtain

$$C(\mu_1,\mu_2,\mu_3) := \overline{\tilde{Y}^Z} - \frac{(\mu_2^2-\mu_3^2)e^{\mu_1}(\overline{\tilde{Y}^Z} - \tilde{G}^Z_{\mu_1}) - (\mu_1^2-\mu_3^2)e^{\mu_2}(\overline{\tilde{Y}^Z} - \tilde{G}^Z_{\mu_2}) + (\mu_1^2-\mu_2^2)e^{\mu_3}(\overline{\tilde{Y}^Z} - \tilde{G}^Z_{\mu_3})}{(\mu_2^2-\mu_3^2)\mu_1 - (\mu_1^2-\mu_3^2)\mu_2 + (\mu_1^2-\mu_2^2)\mu_3}. \tag{D78}$$

By substituting $\overline{\tilde{Y}^Z} = (1-p_d^{\mathcal{Z}})(\eta_\uparrow - \eta_\downarrow)$ and $\tilde{G}_{\mu_j}$ with Eq. (D68) in the last expression, we obtain

$$C(\mu_1,\mu_2,\mu_3) = (1-p_d^{\mathcal{Z}})(\eta_\uparrow - \eta_\downarrow) - \frac{F}{(\mu_2^2-\mu_3^2)\mu_1 - (\mu_1^2-\mu_3^2)\mu_2 + (\mu_1^2-\mu_2^2)\mu_3}, \tag{D79}$$

where we defined

$$\begin{aligned} F :=&(\mu_2^2-\mu_3^2)e^{\mu_1}\left[(\eta_\uparrow - \eta_\downarrow)(1 - G^Z_{\mu_1,(\eta_2,\eta_2)}) + (1-\eta_2)(G^Z_{\mu_1,(\eta_\downarrow,\eta_\downarrow)} - G^Z_{\mu_1,(\eta_\uparrow,\eta_\uparrow)})\right] \\ &- (\mu_1^2-\mu_3^2)e^{\mu_2}\left[(\eta_\uparrow - \eta_\downarrow)(1 - G^Z_{\mu_2,(\eta_2,\eta_2)}) + (1-\eta_2)(G^Z_{\mu_2,(\eta_\downarrow,\eta_\downarrow)} - G^Z_{\mu_2,(\eta_\uparrow,\eta_\uparrow)})\right] \\ &+ (\mu_1^2-\mu_2^2)e^{\mu_3}\left[(\eta_\uparrow - \eta_\downarrow)(1 - G^Z_{\mu_3,(\eta_2,\eta_2)}) + (1-\eta_2)(G^Z_{\mu_3,(\eta_\downarrow,\eta_\downarrow)} - G^Z_{\mu_3,(\eta_\uparrow,\eta_\uparrow)})\right]. \end{aligned} \tag{D80}$$

Finally, we combine the two upper bounds derived in Eqs. (D77) and (D79) to obtain the final expression [analogous to Eq. (D22)] for our upper bound on the linear combination of yields in Eq. (D67):

$$\begin{aligned} &\overline{(\eta_\uparrow - \eta_\downarrow)Y^Z_{1,(\eta_2,\eta_2)} - (1-\eta_2)(Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)} - Y^Z_{1,(\eta_\uparrow,\eta_\uparrow)}) - (\eta_\uparrow - \eta_\downarrow)p_d^{\mathcal{Z}}} \\ &\quad := \min\left\{(1-p_d^{\mathcal{Z}})(\eta_\uparrow - \eta_\downarrow), C(\mu_2,\mu_3), C(\mu_1,\mu_2,\mu_3)\right\}. \end{aligned} \tag{D81}$$

## APPENDIX E: SIMULATION FORMULAS

In this appendix we report the formulas used to generate the simulations reported in Sec. V.

### 1. High-dimensional time-bin QKD

According to the channel model used for simulating the time-bin QKD protocol (Protocol 1) in Figs. 3 and 4, in the absence of eavesdroppers, the $Z$-basis gain reads

$$G^Z_{\mu_j,(\eta_l,\eta_l)} = 1 - (1-p_d^{\mathcal{Z}})e^{-\mu_j\eta\eta_Z(1-\eta_l)}, \tag{E1}$$

where $\eta$ is the transmittance of the quantum channel. For the $X$-basis gains, we recall that we assumed that the signal arriving at Bob is entirely contained in the detection window $\mathcal{Z}$. Hence, the gains are not affected by the transmittance of the TBS outside the interval $\mathcal{Z}$. Thus,

we get

$$G^{X,\checkmark}_{\mu_j,(\eta_i,\eta_l)} = G^{Z}_{\mu_j,(\eta_i,\eta_i)}\left[1-(1-p_d^{\mathcal{X}})e^{-\mu_j\eta\eta_X\eta_i}\right], \quad \text{(E2)}$$

$$G^{X,\emptyset}_{\mu_j,(\eta_i,\eta_l)} = \left(1-G^{Z}_{\mu_j,(\eta_i,\eta_i)}\right)\left[1-(1-p_d^{\mathcal{X}})e^{-\mu_j\eta\eta_X\eta_i}\right]. \quad \text{(E3)}$$

Instead of modeling noise sources in the quantum channel and in the detectors, we assume that each click caused by a photon detection by the $Z$-basis detector ($X$-basis detector) is affected by a channel-intrinsic QBER of $q_Z$ ($q_X$), while the clicks caused by dark counts are random and hence contribute with an error rate of $1-1/d$. Thus, we obtain the following QBER of the key generation rounds:

$$Q_{Z,\mu_j} = \frac{q_Z(1-e^{-\mu_j\eta\eta_Z(1-\eta_\downarrow)}) + \left(1-\frac{1}{d}\right)p_d^{\mathcal{Z}}e^{-\mu_j\eta\eta_Z(1-\eta_\downarrow)}}{G^{Z}_{\mu_j,(\eta_\downarrow,\eta_\downarrow)}}. \quad \text{(E4)}$$

Similarly, the QBERs of the test rounds are given by

$$Q_{X,\mu_j,(\eta_i,\eta_\uparrow),\checkmark} = \frac{q_X(1-e^{-\mu_j\eta\eta_X\eta_i}) + \left(1-\frac{1}{d}\right)p_d^{\mathcal{X}}e^{-\mu_j\eta\eta_X\eta_i}}{1-(1-p_d^{\mathcal{X}})e^{-\mu_j\eta\eta_X\eta_i}}, \quad \text{(E5)}$$

$$Q_{X,\mu_j,(\eta_i,\eta_\uparrow),\emptyset} = Q_{X,\mu_j,(\eta_i,\eta_\uparrow),\checkmark}, \quad \text{(E6)}$$

where we observe that in our error model the test round QBERs are independent of whether the $Z$-basis detector clicks or does not click.

The quantities appearing in the decoy-BB84 key rate (43) are obtained with a standard application of the decoy-state method (see Appendix D). In particular, we have

$$\overline{e_{X,1}} = \min\left\{1, \frac{e^{\mu_2}Q_{X,\mu_2}G^{X}_{\mu_2} - e^{\mu_3}Q_{X,\mu_3}G^{X}_{\mu_3}}{\underline{Y^X_1}(\mu_2-\mu_3)}\right\} \quad \text{(E7)}$$

for the bit error rate upper bound, while the lower bounds on the one-photon yields $\underline{Y^X_1}$ and $\underline{Y^Z_1}$ are reported in Eq. (D11). The lower bound $\underline{Y^Z_0}$ is given by Eq. (D10). Note that these formulas need to be evaluated with the appropriate $Z$-basis or $X$-basis gains. Indeed, in Sec. V we argued that even in the honest implementation of the protocol there is an asymmetry in the gains of the two bases due to asymmetric detectors. We derive the gains appearing in Eq. (43) as follows:

$$G^{Z}_{\mu_j} = G^{Z}_{\mu_j,(\eta_\downarrow,\eta_\downarrow)}, \quad \text{(E8)}$$

$$G^{X}_{\mu_j} = G^{X,\checkmark}_{\mu_j,(\eta_\uparrow,\eta_\uparrow)} + G^{X,\emptyset}_{\mu_j,(\eta_\uparrow,\eta_\uparrow)}, \quad \text{(E9)}$$

where the gains on the right-hand side are given in Eqs. (E1)–(E3). This is because the TBS is not needed in the decoy-BB84 proof; hence, its only use in that protocol is to select the measurement basis, with setting $(\eta_\downarrow,\eta_\downarrow)$ that selects the $Z$ basis and setting $(\eta_\uparrow,\eta_\uparrow)$ that selects the $X$ basis. For the QBERs appearing in Eq. (43), we have

$$Q_{Z,\mu_j} = \frac{q_Z(1-e^{-\mu_j\eta\eta_Z(1-\eta_\downarrow)}) + \left(1-\frac{1}{d}\right)p_d^{\mathcal{Z}}e^{-\mu_j\eta\eta_Z(1-\eta_\downarrow)}}{G^{Z}_{\mu_j}}, \quad \text{(E10)}$$

$$Q_{X,\mu_j} = \frac{q_X(1-e^{-\mu_j\eta\eta_X\eta_\uparrow}) + \left(1-\frac{1}{d}\right)p_d^{\mathcal{X}}e^{-\mu_j\eta\eta_X\eta_\uparrow}}{G^{X}_{\mu_j}}. \quad \text{(E11)}$$

### 2. Attack-induced efficiency mismatch

To study the attack presented in Sec. V B, we assume that Alice can deterministically send one-photon pulses in each round. This allows us to simplify our proof by removing the decoy-state method, which is no longer needed since in this setting one-photon yields and error rates are directly observable quantities.

Here we report the new expressions for the one-photon yields and error rates that enter our key rate (44) and the BB84 key rate (45) when Alice sends one-photon pulses.

#### *a. Protocol statistics without Eve's attack*

First we present the formulas for the case where there is no attack by Eve where and Alice and Bob are linked by a channel with transmittance $\eta$ and intrinsic QBERs $q_Z$ and $q_X$. The one-photon yields are

$$Y^{Z,\mathrm{hon}}_{1,(\eta_l,\eta_l)} = \eta(1-\eta_l)\eta_Z + [1-\eta(1-\eta_l)\eta_Z]p_d^{\mathcal{Z}}, \quad \text{(E12)}$$

$$Y^{X,\mathrm{hon}}_{1,(\eta_l,\eta_l)} = \eta\eta_l\eta_X + [1-\eta\eta_l\eta_X]p_d^{\mathcal{X}}, \quad \text{(E13)}$$

$$\begin{aligned} Y^{X,\checkmark,\mathrm{hon}}_{1,(\eta_i,\eta_l)} &= \eta\eta_i\eta_X p_d^{\mathcal{Z}} + \eta(1-\eta_i)\eta_Z p_d^{\mathcal{X}} \\ &\quad + p_d^{\mathcal{Z}}p_d^{\mathcal{X}}\left[1-\eta+\eta\eta_i(1-\eta_X)\right. \\ &\quad \left.+\,\eta(1-\eta_i)(1-\eta_Z)\right], \end{aligned} \quad \text{(E14)}$$

$$\begin{aligned} Y^{X,\emptyset,\mathrm{hon}}_{1,(\eta_i,\eta_l)} &= (1-p_d^{\mathcal{Z}})\left[\eta\eta_i\eta_X + \eta\eta_i(1-\eta_X)p_d^{\mathcal{X}}\right. \\ &\quad \left.+\,\eta(1-\eta_i)(1-\eta_Z)p_d^{\mathcal{X}} + (1-\eta)p_d^{\mathcal{X}}\right]. \end{aligned} \quad \text{(E15)}$$

The one-photon error rates satisfy the following equalities:

$$\begin{aligned} Y^{Z,\mathrm{hon}}_{1,(\eta_l,\eta_l)}e^{\mathrm{hon}}_{Z,1,(\eta_l,\eta_l)} &= q_Z\eta(1-\eta_l)\eta_Z \\ &\quad + \left(1-\frac{1}{d}\right)[1-\eta(1-\eta_l)\eta_Z]p_d^{\mathcal{Z}}, \end{aligned} \quad \text{(E16)}$$

$$\begin{aligned} Y^{X,\mathrm{hon}}_{1,(\eta_l,\eta_l)}e^{\mathrm{hon}}_{X,1,(\eta_l,\eta_l)} &= q_X\eta\eta_l\eta_X \\ &\quad + \left(1-\frac{1}{d}\right)[1-\eta\eta_l\eta_X]p_d^{\mathcal{X}}, \end{aligned} \quad \text{(E17)}$$

$$Y^{X,\checkmark,\mathrm{hon}}_{1,(\eta_i,\eta_l)} e^{\mathrm{hon}}_{X,1,(\eta_i,\eta_l),\checkmark} = q_X \eta\eta_i\eta_X p_d^Z + \left(1-\frac{1}{d}\right)\left(Y^{X,\checkmark,\mathrm{hon}}_{1,(\eta_i,\eta_l)} - \eta\eta_i\eta_X p_d^Z\right), \tag{E18}$$

$$Y^{X,\emptyset,\mathrm{hon}}_{1,(\eta_i,\eta_l)} e^{\mathrm{hon}}_{X,1,(\eta_i,\eta_l),\emptyset} = q_X \eta\eta_i\eta_X (1-p_d^Z) + \left(1-\frac{1}{d}\right)\left(Y^{X,\emptyset,\mathrm{hon}}_{1,(\eta_i,\eta_l)} - \eta\eta_i\eta_X (1-p_d^Z)\right), \tag{E19}$$

where the yields appearing on the right-hand side are given in Eqs. (E14) and (E15).

By using Eqs. (E12)–(E19) to replace the corresponding bounds in the phase error rate upper bound (B1), we obtain significant simplifications compared with the expressions in Appendix B, which are obtained when Alice prepares phase-randomized coherent pulses for the decoy-state method. In particular, thanks to the knowledge of the true value of the one-photon yields, the estimation of the weight of Bob's received state in the ($\leq 1$)-subspace becomes tight. Namely, the upper bound in Eq. (B5) becomes null ($\overline{w}_Z^{>1} = 0$) once we replace the yields with Eq. (E12). This fact greatly improves the tightness of our key rate bound, so much so that it coincides with the asymptotic key rate of the BB84 protocol without decoys, as shown in Fig. 5, for $w_Z = 0$.

### *b. Protocol statistics with Eve's attack*

Eve intercepts and measures Alice's pulses in the $Z$ basis ($X$ basis) with probability $w_Z$ ($w_X$). Eve can perfectly distinguish Alice's symbols when guessing the right basis. She then prepares a tailored time pulse (frequency pulse), corresponding to the $Z$-basis ($X$-basis) outcome she observed, and sends it through a pure-loss channel with transmittance $\xi_Z$ ($\xi_X$). Her goal is to make her attack undetectable in the standard BB84 protocol. In other words, she aims to introduce little noise in the events where Alice, Bob, and Eve choose the same basis, while decreasing the detection probability at Bob for the events where she chooses the wrong basis, thereby keeping the QBERs low.

Before describing Eve's attack, we review Bob's measurement apparatus for the case of one-photon signals. Bob's measurement apparatus comprises the TBS with setting $(\eta_i, \eta_l)$, followed by a time-of-arrival measurement in the reflected port with efficiency $\eta_Z$. The measurement returns outcome $j'$ if the photon is detected in the time interval centered at $t_{j'}$ with width $\Delta_j$ for each bin. The total detection window in the $Z$ basis is $\Delta_t = d\Delta_j$. The photon transmitted by the TBS undergoes dispersion in a dispersive medium, modeled by the unitary:

$$U_{\mathrm{dis}} = \int_{-\infty}^{\infty} \mathrm{d}f \; e^{i2\pi^2\Phi_2 f^2} |f\rangle\langle f|, \tag{E20}$$

with $\Phi_2$ the group delay dispersion coefficient of the dispersive medium, followed by a time-of-arrival measurement with efficiency $\eta_X$, where outcome $k'$ corresponds to a detection in the time bin centered at $\tilde{t}_{k'}$ with width $\Delta_k$ for each bin. The total detection window in the $X$ basis is $\Delta_f = d\Delta_k$.

To remain undetected, when intercepting the signal in the $Z$ basis, Eve prepares the following one-photon Gaussian time pulse corresponding to outcome $j$:

$$|E_Z(j)\rangle := \int_{-\infty}^{\infty} \mathrm{d}t \, \frac{e^{-\frac{(t-t_j)^2}{2s^2}}}{\sqrt{\sqrt{\pi}s}} |t\rangle, \tag{E21}$$

where $s$ is a free parameter that Eve can freely tune. Similarly, Eve prepares the following one-photon Gaussian-modulated frequency pulse when intercepting the signal in the $X$ basis, corresponding to outcome $k$:

$$|E_X(k)\rangle := \int_{-\infty}^{\infty} \mathrm{d}f \, \frac{e^{-\frac{f^2}{2\sigma^2}}}{\sqrt{\sqrt{\pi}\sigma}} e^{i(2\pi\tilde{t}_k f - 2\pi^2\Phi_2 f^2)} |f\rangle, \tag{E22}$$

where $\sigma$ is a free parameter. In Eqs. (E21) and (E22), $a_f^\dagger |\mathrm{vac}\rangle = |f\rangle$ ($a_t^\dagger |\mathrm{vac}\rangle = |t\rangle$) represents an unphysical state of a single photon at frequency $f$ (time $t$). It holds that $|t\rangle = \int_{-\infty}^{\infty} \mathrm{d}f e^{2i\pi ft} |f\rangle$.

We now compute the probabilities of Bob obtaining certain outcomes, given that Eve performed the attack in the $Z$ basis, Eq. (E21), or the $X$ basis, Eq. (E22).

The probability that Bob obtains outcome $j'$ in the $Z$ basis, given that Eve sent the pulse corresponding to outcome $j$ in Eq. (E21), is given by

$$\Pr(Z_B = j'|Z_E = j) = (1-\eta_i)\eta_Z \int_{t_{j'}-\Delta_j/2}^{t_{j'}+\Delta_j/2} \mathrm{d}t \frac{e^{-\frac{(t-t_j)^2}{s^2}}}{\sqrt{\pi}s} = \frac{(1-\eta_i)\eta_Z}{2}\left[\mathrm{erf}\left(\frac{t_{j'}-t_j+\Delta_j/2}{s}\right) + \mathrm{erf}\left(\frac{-t_{j'}+t_j+\Delta_j/2}{s}\right)\right], \tag{E23}$$

with $\mathrm{erf}(x) = (2/\sqrt{\pi})\int_0^x \mathrm{d}t e^{-t^2}$ the error function. We observe that Eve can tune the width of her Gaussian pulse, $s$, in order to introduce little noise in the $Z$-basis outcomes. This is achieved by Eve choosing $s \ll \Delta_j$ so that $\Pr(Z = j'|Z = j) \propto \delta_{j'j}$. Note that the probability in Eq. (E23) is computed modulo the transmittance $\xi_Z$ of Eve's channel. The probability that Bob obtains outcome $k'$ in the $X$ basis, given that Eve sent the pulse corresponding to outcome $j$ in Eq. (E21), is given by

$$\begin{aligned}\Pr(X_B = k'|Z_E = j) = \eta_X \int_{\tilde{t}_{k'}-\Delta_k/2}^{\tilde{t}_{k'}+\Delta_k/2} \mathrm{d}t \frac{e^{-\frac{(t-t_j)^2}{s^2+(\Phi_2/s)^2}}}{4\sqrt{\pi}\sqrt{s^2+(\Phi_2/s)^2}} \\ \times \left|2\sqrt{\eta_l} + (\sqrt{\eta_i}-\sqrt{\eta_l})\left[\mathrm{erf}\left(\frac{(1+i)s^2(2t+\Delta_t)+(1-i)(2t_j+\Delta_t)\Phi_2}{4s\sqrt{\Phi_2}\sqrt{s^2-i\Phi_2}}\right)\right.\right. \\ \left.\left. - \mathrm{erf}\left(\frac{(1+i)s^2(2t-\Delta_t)+(1-i)(2t_j-\Delta_t)\Phi_2}{4s\sqrt{\Phi_2}\sqrt{s^2-i\Phi_2}}\right)\right]\right|^2, \end{aligned} \tag{E24}$$

and is also computed modulo the transmittance of Eve's channel, $\xi_X$. We observe that Eve can tune $s$ such that $\Phi_2/s \gg \Delta_f$. In this way, she can reduce the detection probability at Bob when they choose opposite bases. In summary, when intercepting the signal in the $Z$ basis, Eve prepares pulses given by Eq. (E21), with $s$ satisfying both $s \ll \Delta_j$ and $\Phi_2/s \gg \Delta_f$, so that Bob observes little noise in the $Z$-basis detections and a reduced detection probability in the $X$ basis.

The probability that Bob obtains outcome $j'$ in the $Z$ basis, given that Eve sent the pulse corresponding to outcome $k$ in Eq. (E22), is given by

$$\Pr(Z_B = j'|X_E = k) = \frac{(1-\eta_i)\eta_Z}{2}\left[\mathrm{erf}\left(\frac{t_{j'}-\tilde{t}_k+\Delta_j/2}{\sqrt{2}\sigma'}\right) + \mathrm{erf}\left(\frac{-t_{j'}+\tilde{t}_k+\Delta_j/2}{\sqrt{2}\sigma'}\right)\right], \tag{E25}$$

where $\sigma' := \sigma\left|1/(2\sigma^2) + 2i\pi^2\Phi_2\right|/\sqrt{2}\pi$. Note that Eve can increase the value of $\sigma$ such that $\sigma' \gg \Delta_t$, thereby reducing the detection probability in the $Z$ basis. The probability that Bob obtains outcome $k'$ in the $X$ basis, given that Eve sent the pulse corresponding to outcome $k$ in Eq. (E22), is given by

$$\begin{aligned}\Pr(X_B = k'|X_E = k) = \eta_X \int_{\tilde{t}_{k'}-\Delta_k/2}^{\tilde{t}_{k'}+\Delta_k/2} \mathrm{d}t \frac{\sqrt{\pi}\sigma}{2} e^{-4\pi^2\sigma^2(t-\tilde{t}_k)^2} \\ \times \left|2\sqrt{\eta_l} + (\sqrt{\eta_i}-\sqrt{\eta_l})\left[\mathrm{erf}\left(\frac{2t+\Delta_t+8i\pi^2\sigma^2\Phi_2(t-\tilde{t}_k)}{2\sqrt{2\Phi_2}\sqrt{4\pi^2\sigma^2\Phi_2-i}}\right)\right.\right. \\ \left.\left. - \mathrm{erf}\left(\frac{2t-\Delta_t+8i\pi^2\sigma^2\Phi_2(t-\tilde{t}_k)}{2\sqrt{2\Phi_2}\sqrt{4\pi^2\sigma^2\Phi_2-i}}\right)\right]\right|^2. \end{aligned} \tag{E26}$$

Similarly, Eve can increase $\sigma$ to satisfy $(4\pi^2\sigma^2)^{-1/2} \ll \Delta_k$, such that the error introduced in the $X$-basis outcomes is negligible: $\Pr(X_B = k'|X_B = k) \propto \delta_{kk'}$.

Given the attacks described in Eqs. (E21) and (E22), the resulting one-photon yields read

$$Y^Z_{1,(\eta_l,\eta_l)} = (1-w_X-w_Z)Y^{Z,\mathrm{hon}}_{1,(\eta_l,\eta_l)} + w_Z\left[p_d^{\mathcal{Z}} + \xi_Z \Pr(Z\checkmark|Z)(1-p_d^{\mathcal{Z}})\right] + w_X\left[p_d^{\mathcal{Z}} + \xi_X \Pr(Z\checkmark|X)(1-p_d^{\mathcal{Z}})\right], \tag{E27}$$

$$Y^X_{1,(\eta_l,\eta_l)} = (1-w_X-w_Z)Y^{X,\mathrm{hon}}_{1,(\eta_l,\eta_l)} + w_Z\left[p_d^{\mathcal{X}} + \xi_Z \Pr(X\checkmark|Z)(1-p_d^{\mathcal{X}})\right] + w_X\left[p_d^{\mathcal{X}} + \xi_X \Pr(X\checkmark|X)(1-p_d^{\mathcal{X}})\right], \tag{E28}$$

$$\begin{aligned}Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} &= (1-w_X-w_Z)Y^{X,\checkmark,\mathrm{hon}}_{1,(\eta_i,\eta_l)} \\ &+ w_Z\left[\xi_Z \Pr(X\checkmark|Z)p_d^{\mathcal{Z}} + \xi_Z \Pr(Z\checkmark|Z)p_d^{\mathcal{X}} + (1-\xi_Z \Pr(X\checkmark|Z) - \xi_Z \Pr(Z\checkmark|Z))\, p_d^{\mathcal{Z}}p_d^{\mathcal{X}}\right] \\ &+ w_X\left[\xi_X \Pr(X\checkmark|X)p_d^{\mathcal{Z}} + \xi_X \Pr(Z\checkmark|X)p_d^{\mathcal{X}} + (1-\xi_X \Pr(X\checkmark|X) - \xi_X \Pr(Z\checkmark|X))\, p_d^{\mathcal{Z}}p_d^{\mathcal{X}}\right], \end{aligned} \tag{E29}$$

$$\begin{aligned}Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} &= (1-w_X-w_Z)Y^{X,\emptyset,\mathrm{hon}}_{1,(\eta_i,\eta_l)} + w_Z\left[\xi_Z \Pr(X\checkmark|Z)(1-p_d^{\mathcal{Z}}) + (1-\xi_Z \Pr(X\checkmark|Z) - \xi_Z \Pr(Z\checkmark|Z))\, p_d^{\mathcal{X}}(1-p_d^{\mathcal{Z}})\right] \\ &+ w_X\left[\xi_X \Pr(X\checkmark|X)(1-p_d^{\mathcal{Z}}) + (1-\xi_X \Pr(X\checkmark|X) - \xi_X \Pr(Z\checkmark|X))\, p_d^{\mathcal{X}}(1-p_d^{\mathcal{Z}})\right], \end{aligned} \tag{E30}$$

where $\Pr(Z\checkmark|Z)$ is the probability that Bob obtains a detection in the $Z$ basis, given that Eve intercepted the signal in the $Z$ basis. In particular, we have

$$\Pr(Z\checkmark|Z) = \frac{1}{d}\sum_{j,j'=0}^{d-1} \Pr(Z_B = j'|Z_E = j), \tag{E31}$$

where we accounted for the fact that Alice sends uniformly random symbols and that Eve can perfectly distinguish them. Similarly, we have

$$\Pr(X\checkmark|Z) = \frac{1}{d}\sum_{k',j=0}^{d-1} \Pr(X_B = k'|Z_E = j), \tag{E32}$$

where we accounted for the fact that Eve obtains a uniformly random outcome when measuring Alice's pulses in the opposite basis. Analogously, we have

$$\Pr(Z\checkmark|X) = \frac{1}{d}\sum_{k,j'=0}^{d-1} \Pr(Z_B = j'|X_E = k), \tag{E33}$$

$$\Pr(X\checkmark|X) = \frac{1}{d}\sum_{k',k=0}^{d-1} \Pr(X_B = k'|X_E = k). \tag{E34}$$

Finally, the one-photon error rates in the adversarial implementation satisfy

$$\begin{aligned} Y^{Z}_{1,(\eta_l,\eta_l)} e_{Z,1,(\eta_l,\eta_l)} &= (1 - w_Z - w_X) Y^{Z,\mathrm{hon}}_{1,(\eta_l,\eta_l)} e^{\mathrm{hon}}_{Z,1,(\eta_l,\eta_l)} + w_Z \left[\xi_Z \Pr(Z\mathrm{err}|Z) + (1 - \xi_Z \Pr(Z\checkmark|Z))\, p_d^{\mathcal{Z}} \left(1 - \frac{1}{d}\right)\right] \\ &\quad + w_X \left[\xi_X \Pr(Z\mathrm{err}|X) + (1 - \xi_X \Pr(Z\checkmark|X))\, p_d^{\mathcal{Z}} \left(1 - \frac{1}{d}\right)\right], \end{aligned} \tag{E35}$$

$$\begin{aligned} Y^{X}_{1,(\eta_l,\eta_l)} e_{X,1,(\eta_l,\eta_l)} &= (1 - w_Z - w_X) Y^{X,\mathrm{hon}}_{1,(\eta_l,\eta_l)} e^{\mathrm{hon}}_{X,1,(\eta_l,\eta_l)} + w_Z \left[\xi_Z \Pr(X\mathrm{err}|Z) + (1 - \xi_Z \Pr(X\checkmark|Z))\, p_d^{\mathcal{X}} \left(1 - \frac{1}{d}\right)\right] \\ &\quad + w_X \left[\xi_X \Pr(X\mathrm{err}|X) + (1 - \xi_X \Pr(X\checkmark|X))\, p_d^{\mathcal{X}} \left(1 - \frac{1}{d}\right)\right], \end{aligned} \tag{E36}$$

$$\begin{aligned} Y^{X,\checkmark}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\checkmark} &= (1 - w_Z - w_X) Y^{X,\checkmark,\mathrm{hon}}_{1,(\eta_i,\eta_l)} e^{\mathrm{hon}}_{X,1,(\eta_i,\eta_l),\checkmark} + w_Z \left[\xi_Z \Pr(X\mathrm{err}|Z) p_d^{\mathcal{Z}} + \xi_Z \Pr(Z\checkmark|Z) p_d^{\mathcal{X}} \left(1 - \frac{1}{d}\right)\right. \\ &\quad \left. + (1 - \xi_Z \Pr(X\checkmark|Z) - \xi_Z \Pr(Z\checkmark|Z)) p_d^{\mathcal{X}} p_d^{\mathcal{Z}} \left(1 - \frac{1}{d}\right)\right] \\ &\quad + w_X \left[\xi_X \Pr(X\mathrm{err}|X) p_d^{\mathcal{Z}} + \xi_X \Pr(Z\checkmark|X) p_d^{\mathcal{X}} \left(1 - \frac{1}{d}\right)\right. \\ &\quad \left. + (1 - \xi_X \Pr(X\checkmark|X) - \xi_X \Pr(Z\checkmark|X)) p_d^{\mathcal{X}} p_d^{\mathcal{Z}} \left(1 - \frac{1}{d}\right)\right], \end{aligned} \tag{E37}$$

$$\begin{aligned} Y^{X,\emptyset}_{1,(\eta_i,\eta_l)} e_{X,1,(\eta_i,\eta_l),\emptyset} &= (1 - w_Z - w_X) Y^{X,\emptyset,\mathrm{hon}}_{1,(\eta_i,\eta_l)} e^{\mathrm{hon}}_{X,1,(\eta_i,\eta_l),\emptyset} + w_Z \left[\xi_Z \Pr(X\mathrm{err}|Z)(1 - p_d^{\mathcal{Z}})\right. \\ &\quad \left. + (1 - \xi_Z \Pr(X\checkmark|Z) - \xi_Z \Pr(Z\checkmark|Z)) p_d^{\mathcal{X}} (1 - p_d^{\mathcal{Z}}) \left(1 - \frac{1}{d}\right)\right] \\ &\quad + w_X \left[\xi_X \Pr(X\mathrm{err}|X)(1 - p_d^{\mathcal{Z}}) + (1 - \xi_X \Pr(X\checkmark|X) - \xi_X \Pr(Z\checkmark|X)) p_d^{\mathcal{X}} (1 - p_d^{\mathcal{Z}}) \left(1 - \frac{1}{d}\right)\right], \end{aligned} \tag{E38}$$

where $\Pr(Z\text{err}|Z)$ is the probability that Bob obtains a click in the $Z$ basis and the outcome is different from Alice's, given that Eve attacked in the same basis:

$$\Pr(Z\text{err}|Z) = \frac{1}{d}\sum_{j=0}^{d-1}\sum_{j'\neq j}\Pr(Z_B = j'|Z_E = j), \tag{E39}$$

where again we assumed that Eve can perfectly distinguish Alice's symbols with no errors when she chooses the same basis. When Eve chooses the opposite basis, the probability that Bob gets an error is given by

$$\begin{aligned}\Pr(Z\text{err}|X) &= \frac{1}{d}\sum_{j,k=0}^{d-1}\sum_{j'\neq j} \\ &\quad\times \Pr(Z_B = j'|X_E = k)\Pr(X_E = k|Z_A = j) \\ &= \frac{1}{d^2}\sum_{j,k=0}^{d-1}\sum_{j'\neq j}\Pr(Z_B = j'|X_E = k),\end{aligned} \tag{E40}$$

where we used the fact that Eve's outcome is uniformly random when measuring in the basis opposite Alice's. In the same vein, we have

$$\Pr(X\text{err}|X) = \frac{1}{d}\sum_{k=0}^{d-1}\sum_{k'\neq k}\Pr(X_B = k'|X_E = k), \tag{E41}$$

$$\Pr(X\text{err}|Z) = \frac{1}{d^2}\sum_{j,k=0}^{d-1}\sum_{k'\neq k}\Pr(X_B = k'|Z_E = j). \tag{E42}$$

### *c. Upper bound on secret key rate*

Here we derive the upper bound on the asymptotic secret key rate achievable by Alice and Bob under Eve's attack. The upper bound is plotted in Fig. 5 together with the BB84 key rate. The fact that the latter surpasses the former indicates that the BB84 protocol is insecure and returns overly optimistic key rates, as discussed in Sec. VI.

The upper bound is obtained by considering the raw key bits per pulse shared by Alice and Bob, $r_{\text{raw}}$, and by subtracting the number of raw key bits per pulse known to Eve, $r_{\text{Eve}}$. For $r_{\text{raw}}$, we have

$$r_{\text{raw}} = p_Z^2 Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}\log_2 d, \tag{E43}$$

since the key bits are generated only from the events where both Alice and Bob choose the $Z$ basis and Bob gets a detection. The factor $\log_2 d$ accounts for the fact that each symbol contains $\log_2 d$ bits of information. For $r_{\text{Eve}}$, we recall that Eve knows perfectly the shared raw key bits in the rounds where Alice, Bob, and Eve all choose the $Z$ basis and Bob gets a detection in the $Z$ basis. Moreover, Eve learns the bits exchanged by Alice and Bob for error correction. This amounts to the following rate of raw key bits known to Eve:

$$\begin{aligned}r_{\text{Eve}} &= p_Z^2 w_Z\left[p_d^{\mathcal{Z}} + \xi_Z \Pr(Z\checkmark|Z)(1-p_d^{\mathcal{Z}})\right]\log_2 d \\ &\quad + p_Z^2 Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)} u(e_{Z,1,(\eta_\downarrow,\eta_\downarrow)}).\end{aligned} \tag{E44}$$

Hence, the upper bound on the secret key rate is given by

$$\begin{aligned}r_{\text{raw}} - r_{\text{Eve}} &= p_Z^2 Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}\left[\log_2 d - u(e_{Z,1,(\eta_\downarrow,\eta_\downarrow)})\right] \\ &\quad - p_Z^2 w_Z\left[p_d^{\mathcal{Z}} + \xi_Z \Pr(Z\checkmark|Z)(1-p_d^{\mathcal{Z}})\right]\log_2 d.\end{aligned} \tag{E45}$$

### 3. Secret key rate versus (mode-independent) detection efficiency mismatch

In this section, we study the performance of the key rate from our proof, Eq. (17), for various asymmetries in the mode-independent detection efficiency of the two bases, i.e., as a function of $\eta_r = \eta_X/\eta_Z$. This study stems from the observation made in Sec. VI that our key rate does not match the decoy-BB84 key rate in the case of an honest implementation of the protocol and that the difference may be due to the asymmetric detection efficiency of the two bases.

In Fig. 8, we plot the key rate (17) as a function of $\eta_r$ and compare it with the decoy-BB84 rate (43) and with the same key rate (17) obtained by our artificially setting the weight of the state received by Bob outside the

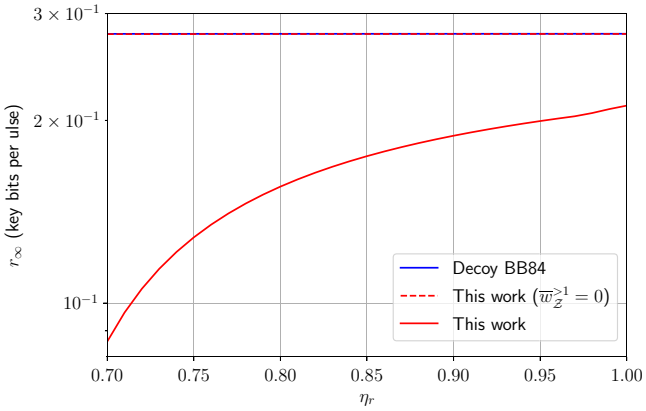


FIG. 8. The secret key rate in Eq. (17) in the case of the honest implementation in Sec. V A as a function of the detection efficiency mismatch $\eta_r$. Note that we fix $\eta_Z = 0.9\times10^{-1/10}$ and vary $\eta_X$ to achieve different values of $\eta_r$. We also fix the intrinsic QBERs to $q_Z = q_X = 0.02$. The solid red line represents the secure key rate obtained with the bound on $\overline{w}^{>1}_{\mathcal{Z}}$ reported in Eq. (B5). The dashed red line represents the key rate when we impose $\overline{w}^{>1}_{\mathcal{Z}} = 0$. The solid blue line represents the decoy-BB84 key rate in Eq. (43). We observe that the dashed red line perfectly overlaps the solid blue line, indicating that our proof will become tight and match the decoy-BB84 rate when a tight estimation of $\overline{w}^{>1}_{\mathcal{Z}}$ is available.

($\leq 1$)-subspace to zero: $\overline{w}_{\mathcal{Z}}^{>1} = 0$. This would correspond to the scenario with perfect knowledge of the parameter $\overline{w}_{\mathcal{Z}}^{>1}$, which is indeed null in the honest implementation considered . The other parameters are set as in Fig. 4 for the honest implementation of the protocol, where $\eta_Z = 0.9 \times 10^{-1/10}$ and the channel loss $\eta$ is fixed to $10^{-1/10}$.

From Fig. 8, we observe that in the case of perfect knowledge of the parameter $\overline{w}_{\mathcal{Z}}^{>1}$, the detection efficiency mismatch does not influence the key rate (17) and the latter matches the decoy-BB84 key rate perfectly. Conversely, when our bound, Eq. (B5), is used on the parameter $\overline{w}_{\mathcal{Z}}^{>1}$, the key rate of our proof presents a gap to the decoy-BB84 rate that increases as $\eta_r$ decreases. Therefore, we deduce that the nontight estimation of $\overline{w}_{\mathcal{Z}}^{>1}$ is the main cause of loss of performance, becoming more problematic as the asymmetry in the detection efficiencies increases.


[1] Inside Quantum Technology, Quantum key distribution (QKD) markets: 2019–2028. https://www.insidequantumtechnology.com/product/quantum-key-distribution-qkd-markets-2019-2028 [Online].

[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photon. **12**, 1012 (2020).

[3] French Cybersecurity Agency (ANSSI), Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), and Swedish National Communications Security Authority (Swedish NCSA), Position paper on quantum key distribution (2024).

[4] M. Lucamarini, A. Shields, R. Alléaume, C. Chunnilall, I. P. Degiovanni, M. Gramegna, A. Hasekioglu, B. Huttner, R. Kumar, A. Lord, N. Lütkenhaus, V. Makarov, V. Martin, A. Mink, M. Peev, M. Sasaki, A. Sinclair, T. Spiller, M. Ward, C. White, and Z. Yuan, Implementation security of quantum cryptography, *ETSI White Paper No. 27*, (2018).

[5] V. Zapatero, A. Navarrete, and M. Curty, Implementation security in quantum key distribution, Adv. Quantum Technol. **8**, 2300380 (2024).

[6] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[7] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. **85**, 441 (2000).

[8] M. Tomamichel and A. Leverrier, A largely self-contained and complete security proof for quantum key distribution, Quantum **1**, 14 (2017).

[9] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A **89**, 022307 (2014).

[10] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Loss-tolerant quantum cryptography with imperfect sources, Phys. Rev. A **90**, 052314 (2014).

[11] M. K. Bochkov and A. S. Trushechkin, Security of quantum key distribution with detection-efficiency mismatch in the single-photon case: Tight bounds, Phys. Rev. A **99**, 032308 (2019).

[12] A. Trushechkin, Security of quantum key distribution with detection-efficiency mismatch in the multiphoton case, Quantum **6**, 771 (2022).

[13] J. Nunn, L. J. Wright, C. Söller, L. Zhang, I. A. Walmsley, and B. J. Smith, Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion, Opt. Express **21**, 15959 (2013).

[14] J. E. Bourassa and H.-K. Lo, Entropic uncertainty relations and the measurement range problem, with consequences for high-dimensional quantum key distribution, J. Opt. Soc. Am. B **36**, B65 (2019).

[15] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photon. **4**, 686 (2010).

[16] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, Phys. Rev. A **78**, 042333 (2008).

[17] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch, Phys. Rev. A **91**, 062301 (2015).

[18] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Simple 2.5 GHz time-bin quantum key distribution, Appl. Phys. Lett. **112**, 171108 (2018).

[19] I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D. Bacco, Efficient time-bin encoding for practical high-dimensional quantum key distribution, Phys. Rev. Appl. **14**, 014051 (2020).

[20] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Provably secure and high-rate quantum key distribution with time-bin qudits, Sci. Adv. **3**, e1701491 (2017).

[21] N. T. Islam, C. C. W. Lim, C. Cahall, B. Qi, J. Kim, and D. J. Gauthier, Scalable high-rate, high-dimensional time-bin encoding quantum key distribution, Quantum Sci. Technol. **4**, 035008 (2019).

[22] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, High-dimensional quantum key distribution using dispersive optics, Phys. Rev. A **87**, 062322 (2013).

[23] C. Lee, D. Bunandar, Z. Zhang, G. R. Steinbrecher, P. B. Dixon, F. N. C. Wong, J. H. Shapiro, S. A. Hamilton, and D. Englund, Large-alphabet encoding for higher-rate quantum key distribution, Opt. Express **27**, 17539 (2019).

[24] J. Rödiger, N. Perlot, R. Mottola, R. Elschner, C.-M. Weinert, O. Benson, and R. Freund, Numerical assessment and optimization of discrete-variable time-frequency quantum key distribution, Phys. Rev. A **95**, 052312 (2017).

[25] Y. Zhang, I. B. Djordjevic, and M. A. Neifeld, Weak-coherent-state-based time-frequency quantum key distribution, J. Mod. Opt. **62**, 1713 (2015).

[26] M. Leifgen, R. Elschner, N. Perlot, C. Weinert, C. Schubert, and O. Benson, Practical implementation and evaluation of a quantum-key-distribution scheme based on the time-frequency uncertainty, Phys. Rev. A **92**, 042311 (2015).
[27] K.-C. Chang, M. C. Sarihan, X. Cheng, Z. Zhang, and C. W. Wong, Large-alphabet time-bin quantum key distribution and Einstein-Podolsky-Rosen steering via dispersive optics, Quantum Sci. Technol. **9**, 015018 (2024).
[28] T. Moroder, M. Curty, and N. Lütkenhaus, Detector decoy quantum key distribution, New J. Phys. **11**, 045008 (2009).
[29] A. Widomski, M. Ogrodnik, and M. Karpiński, Efficient detection of multidimensional single-photon time-bin superpositions, Optica **11**, 926 (2024).
[30] M. Ogrodnik, A. Widomski, D. Bruß, G. Chesi, F. Grasselli, H. Kampermann, C. Macchiavello, N. Walk, N. Wyderka, and M. Karpiński, High-dimensional quantum key distribution with resource-efficient detection, arXiv:2412.16782.
[31] Federal Office for Information Security (BSI), Implementation attacks against QKD systems (2023).
[32] M. Zahidy, D. Ribezzo, C. De Lazzari, I. Vagniluca, N. Biagi, R. Müller, T. Occhipinti, L. K. Oxenløwe, M. Galili, T. Hayashi, D. Cassioli, A. Mecozzi, C. Antonelli, A. Zavatta, and D. Bacco, Practical high-dimensional quantum key distribution protocol over deployed multicore fiber, Nat. Commun. **15**, 1651 (2024).
[33] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Security proof of quantum key distribution with detection efficiency mismatch, Quantum Inf. Comput. **9**, 131 (2009).
[34] J. Ma, Y. Zhou, X. Yuan, and X. Ma, Operational interpretation of coherence in quantum key distribution, Phys. Rev. A **99**, 062325 (2019).
[35] L. Lydersen and J. Skaar, Security of quantum key distribution with bit and basis dependent detector flaws, Quantum Inf. Comput. **10**, 60 (2010).
[36] 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).
[37] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).
[38] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. **94**, 230503 (2005).
[39] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).
[40] X.-S. Ma, S. Zotter, N. Tetik, A. Qarry, T. Jennewein, and A. Zeilinger, A high-speed tunable beam splitter for feed-forward photonic quantum information processing, Opt. Express **19**, 22723 (2011).
[41] R. R. Carreira, J. J. Barroso, and J. E. B. Oliveira, Generalized analysis of dual-output Mach-Zehnder modulator with applications to photonic-assisted instantaneous frequency measurement, J. Lightwave Technol. **39**, 7956 (2021).
[42] M. Christandl, R. König, and R. Renner, Postselection technique for quantum channels with applications to quantum cryptography, Phys. Rev. Lett. **102**, 020504 (2009).
[43] S. Nahar, D. Tupkary, Y. Zhao, N. Lütkenhaus, and E. Y.-Z. Tan, Postselection technique for optical quantum key distribution with improved de Finetti reductions, PRX Quantum **5**, 040315 (2024).
[44] M. Y. Niu, F. Xu, J. H. Shapiro, and F. Furrer, Finite-key analysis for time-energy high-dimensional quantum key distribution, Phys. Rev. A **94**, 052323 (2016).
[45] N. Walk, J. Barrett, and J. Nunn, Composably secure time-frequency quantum key distribution, arxiv:1609.09436.
[46] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc.: Math., Phys. Eng. Sci. **461**, 207 (2005).
[47] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, Phys. Rev. Lett. **91**, 057901 (2003).
[48] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, The uncertainty principle in the presence of quantum memory, Nat. Phys. **6**, 659 (2010).
[49] M. Tomamichel and R. Renner, Uncertainty relation for smooth entropies, Phys. Rev. Lett. **106**, 110506 (2011).
[50] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks, Phys. Rev. Lett. **109**, 100502 (2012).
[51] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, Position-momentum uncertainty relations in the presence of quantum memory, J. Math. Phys. **55**, 122205 (2014).
[52] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, Cambridge, 2011).
[53] In an adversarial implementation, we cannot discard the possibility that Eve adds photons to Alice's pulse before it reaches Bob.
[54] D. Tupkary, S. Nahar, P. Sinha, and N. Lütkenhaus, Phase error rate estimation in QKD with imperfect detectors, arXiv:2408.17349.
[55] A. Winick, N. Lütkenhaus, and P. J. Coles, Reliable numerical key rates for quantum key distribution, Quantum **2**, 77 (2018).
[56] Y. Zhang and N. Lütkenhaus, Entanglement verification with detection-efficiency mismatch, Phys. Rev. A **95**, 042319 (2017).
[57] S. Nahar, T. Upadhyaya, and N. Lütkenhaus, Imperfect phase randomization and generalized decoy-state quantum key distribution, Phys. Rev. Appl. **20**, 064031 (2023).
[58] R. Bhatia and C. Davis, A Cauchy-Schwarz inequality for operators with applications, Linear Algebra Appl. **223–224**, 119 (1995), Honoring Miroslav Fiedler and Vlastimil Ptak.