arXiv:2408.17349v4 [quant-ph] 3 Dec 2025

Phase error rate estimation in QKD with imperfect detectors

Devashish Tupkary[1], Shlok Nahar[1], Pulkit Sinha[2], and Norbert Lütkenhaus[1]

[1]Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1

[2]Institute for Quantum Computing and School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1

We present a finite-size security proof of the decoy-state BB84 QKD protocol against coherent attacks, using entropic uncertainty relations, for imperfect detectors. We apply this result to the case of detectors with imperfectly characterized basis-efficiency mismatch. Our proof works by obtaining a suitable bound on the phase error rate, without requiring any new modifications to the protocol steps or hardware. It is applicable to imperfectly characterized detectors, and only requires the maximum relative difference in detection efficiencies and dark count rates of the detectors to be characterized. Moreover, our proof allows Eve to choose detector efficiencies and dark count rates in their allowed ranges in each round, thereby addressing an important problem of detector side channels. We prove security in the variable-length framework, where users are allowed to adaptively determine the length of key to be produced, and number of bits to be used for error-correction, based on observations made during the protocol. We quantitatively demonstrate the effect of basis-efficiency mismatch by applying our results to the decoy-state BB84 protocol.

1 Introduction

Security proofs of QKD based on the entropic uncertainty relations (EUR) [1–4], and the phase error correction approach [4–6], yield some of the highest key rates against coherent attacks in the finite-size regime. While source imperfections [7–10] have been extensively studied within the phase error correction framework, detector imperfections have not yet been addressed in any meaningful sense in either security proof framework. In particular, these proof techniques require the probability of detection in Bob's detection setup to be independent of basis choice. This assumption is referred to as "basis-independent loss" in the literature, while the violation of this assumption is referred to as "basis-efficiency mismatch" or "detection-efficiency mismatch". Satisfying this assumption requires the efficiency and dark count rates of Bob's detectors to be *exactly* identical. Therefore, justifying this assumption in practice requires *exact* characterization of Bob's identical detectors. Either of these tasks are impossible in practice. Therefore, these proof techniques are not applicable to practical prepare-and-measure (and entangled-based) QKD scenarios involving realistic detectors. Note that MDI-QKD [11] is able to address *all* detector imperfections and detector side-channels, since it assumes the detectors to be completely in Eve's control. Morever, source imperfections can also be handled to a large degree. However, MDI-QKD is significantly more complex to implement as compared to prepare-and-measure QKD, and the latter remain dominant in real-world implementations. Thus, addressing detector imperfections within prepare-and-measure QKD is of paramout importance. To date, there is no security proof method that addresses this problem *without* requiring significant protocol modifications. While some theoretical analyses of basis-efficiency mismatch in the asymptotic setting exist for standard QKD [12–16], there is no work that handles basis-efficiency mismatch for coherent attacks in the finite-size regime. Meanwhile,

Devashish Tupkary: djtupkary@uwaterloo.ca
Norbert Lütkenhaus: nlutkenhaus.office@uwaterloo.ca

there have been several experimental demonstrations [17–21], exploiting basis-efficiency mismatch for attacks on QKD systems.

In this work, we prove the security of the decoy-state BB84 protocol with an active detection setup *without* assuming basis-independent loss. We do so by showing that the phase error rate can be suitably bounded even without the assumption. We explicitly define metrics δ_1, δ_2 that quantify the deviation from the ideal case, and bound the phase error rate in terms of these deviations. Our framework is general, and can be applied to any (IID) detector model of one's choice, as long as the relevant metrics δ_1, δ_2 can be suitable bounded. In general, this will require some model of the detectors and characterization of its properties. An important, non-trivial open question remains on how best to experimentally bound these quantities. We leave a full experimental analysis for future work, and restrict our attention in this work to the case where we utilise common models for detectors [1], and bound δ_1, δ_2 in terms of commonly measured model parameters [22].

In this work we explicitly compute these metrics for the case of detectors with basis-efficiency mismatch and unequal dark count rates. To do so, we assume the the canonical model of detectors described in Section 6.3. The block-diagonal structure of the detector POVMs significantly aids the computation of these metrics. Moreover, we compute these metrics directly from the experimental characterization of the detection efficiencies and dark count rates of the detectors. Our results extend the security of QKD to the following practical scenarios:

1. Bob's detectors are *not* identical, but the values of efficiency (η_{b_i} for basis b and outcome i) and dark count rates (d_{b_i}) are known. Note that while this is a useful toy model, such scenarios are impractical since they require η_{b_i}, d_{b_i} to be known exactly. We treat the dark count rate as a part of the POVM element, as described in Section 6.3.

2. Bob's detectors are *not* identical, and the values of efficiency and dark count rates are only known to be in some range $\eta_{b_i} \in [\eta_{\text{det}}(1-\Delta_\eta), \eta_{\text{det}}(1+\Delta_\eta)], d_{b_i} \in [d_{\text{det}}(1-\Delta_{\text{dc}}), d_{\text{det}}(1+\Delta_{\text{dc}})]$. While this is again a useful toy model, a detectors response (η_{b_i}, d_{b_i}) to incoming photons typically depends on the spatio-temporal modes of incoming photons, which are in Eve's control.

3. Bob's detectors are *not* identical, and the values of efficiency and dark count rates are only known to be in some range. Moreover, these values depend on the spatio-temporal modes (labelled by $\mathbf{d}$) of the incoming photons, and can therefore be chosen by Eve [14, 18, 20, 21]. This is expressed mathematically as $\eta_{b_i}(\mathbf{d}) \in [\eta_{\text{det}}(\mathbf{d})(1-\Delta_\eta), \eta_{\text{det}}(\mathbf{d})(1+\Delta_\eta)], d_{b_i}(\mathbf{d}) \in [d_{\text{det}}(1-\Delta_{\text{dc}}), d_{\text{det}}(1+\Delta_{\text{dc}})]$. Note that in this model, the range of allowed values of the loss can depend on the spatio-temporal mode, whereas the dark count rates for all the modes lie in the same range.

Our metrics δ_1, δ_2 involve an optimization over all possible values of η_{b_i}, d_{b_i} in their respective ranges. Moreover, for our model of multi-mode detectors, we find that our methods yield the same values for Case 2 and Case 3. Thus, our methods address one practically important detector side-channel as a by-product. We discuss this in greater detail in Section 8.

We use entropic uncertainty relations [1] for our security proofs in this work. Since both the entropic uncertainty relations approach and the phase error correction [5, 6] approach involve bounding the phase error rate, we expect our techniques to also work when using the phase error correction approach for the security proof. In fact, one may also use the equivalence by Tsurumuru [23, 24] to relate the two security proof approaches. For example, [24, Section III] constructs an explicit phase error correction circuit whose failure probability can be bound by the smooth min entropy via [24, Theorem 1 and Corollary 2]. Therefore one may indirectly prove security in the phase error correction framework by applying the above equivalence on the results of this work.

Moreover, we prove security in the variable-length framework [25, 26] which allows Alice and Bob to adaptively determine the number of bits to be used for error-correction, and the length of the output key, based on the observations during runtime. Such protocols are critical for practical

[1] We stress that characterisation will *always* proceed by assuming some physically motivated model of the devices in terms of a small number of paramters. The characterisation experiment will then estimate these model parameters. The question that must then be answered is about which model best describes the physical implementation, and how to characterise the parameters of the chosen model.

implementations, where the honest behavior of the channel connecting Alice and Bob is difficult to determine in advance. A security proof for variable-length QKD has been recently obtained for generic protocols in Ref. [27] which utilizes an IID security proof followed by the postselection technique lift [28, 29] to coherent attacks. The use of the postselection technique in Ref. [27] leads to pessimistic key rates, which is avoided by this work. Our proof of variable-length security uses the same essential tricks as prior work on variable-length security in Refs. [30] and [31, Chapter 3] for the phase error correction framework, and is nearly identical to [32, Supplementary Note A] for the EUR framework.

This paper is organized as follows. We discuss similarities and differences with other related work [12–16, 33, 34] towards the end of this section. In Section 2, we describe the QKD protocol that we consider in this work. For simplicity, we first consider the BB84 protocol where Alice prepares perfect single-photon signal states. We do this since there are many existing techniques for dealing with imperfect state preparation by Alice, and the goal of this work is to focus on detector imperfections. We show that that the variable-length security of the QKD protocol follows if one is able to obtain suitable bounds on the phase error rate (Eq. (5)). In Section 3 we show how such bounds can be obtained in the case where the basis-independent loss assumption is satisfied. In Section 4, we show how such bounds can be obtained in scenarios where the basis-independent loss assumption is *not* satisfied. In Section 5 we extend our analysis to prove the variable-length security of the decoy-state BB84 protocol with imperfect detectors. In Section 6 we apply our results and compute key rates for the decoy-state BB84 protocol, and study the impact of basis-efficiency mismatch on key rates. We base our analysis of decoy-state BB84 on Lim et al [35], and also point out and fix a few technical issues in that work. In Section 7 we outline an approach towards addressing correlated detectors. In Section 8 we explain how our results can be applied to detector side channels (Case. 3 above). In Section 9 we summarize and present concluding remarks. Many details are relegated to the Appendices.

Thus, in this work we

1. Provide a method for phase error rate estimation in the presence of (bounded) detector imperfections, in the finite-size setting against coherent attacks.

2. Address some detector side-channel vulnerabilities by allowing Eve to control (bounded) detector imperfections.

3. Rigorously prove the variable-length security of the decoy-state BB84 protocol in the framework of entropic uncertainty relations.

We have attempted to write this paper in a largely modular fashion beyond Section 2. For variable-length security, one can directly read Sections B and 5.5. Similarly, for phase error estimation for the BB84 protocol, one can directly read Section 3 (for perfect detectors) and Section 4 (for imperfect detectors). For phase error estimation in decoy-state BB84, one can read Sections 5.2 and 5.3. For a recipe for applying our results to compute key rates in the presence of detector imperfections, one can refer to Section 6.1. For the application of our results to detectors with efficiency mismatch, one can refer to Sections 6.3 to 6.5. Sections 7 and 8 can be read independently, but require Section 4 to be read first.

1.1 Relation to other work on basis-efficiency mismatch

Paper	Coherent Attacks	Finite-size	Eve has (bounded) control over detectors	Hardware Modifications	Notes
Fung et al. [13]	Yes	No	Yes	Detector Decoy [36] (To remove Qubit assumption)	-
Lydersen et al. [12]	Yes	No	Yes	None	Handles wide range of multi-mode models
Øystein Marøy et al. [33]	Yes	No	Yes	None	Handles wide range of multi-mode models
Winick et al. [37]	No	No	No	None	-
Zhang et al. [14]	No	No	Yes*	None	* Only two modes
Bochkov et al. [15]	No	No	No	None	Qubit assumption on Bob
Trushechkin et al. [16]	No	No	No	None	-
Grasselli et al. [38]	No	No	No	Detector decoy [36], requires tunable beam splitter	Does not require detector characterization
Marcomini et al. [34]	Yes	No	No	No	Qubit assumption Bob, can handle some source imperfections.
This work	Yes	Yes	Yes	None	

Table 1: Comparison of prior work on phase error rate estimation in the presence of basis efficiency mismatch. Note that Ref. [14] relies on numerical evidence for a part of the proof (bounding weight outside the subspace of low photon numbers).

We will now discuss several prior works on addressing basis-efficiency mismatch in the literature (see Table 1). In a broad sense, the technique used in this work of reformulating the detector setup as first implementing a filtering step followed by further measurements is an important ingredient in many of these works (although the precise details may differ). However, all of them perform an asymptotic analysis, where there is no need for finite-size sampling arguments we use (such as Lemmas 2 and 3 of this work). Instead one can directly associate the various error rates with POVM measurements on a single round state, and the analysis is greatly simplified.

Ref. [13] proposed the first security proof of QKD in the presence of (bounded) Eve controlled basis-efficiency mismatch, in the asymptotic regime. It required the assumption that a qubit is received on Bob's side, for which it required the use of detector-decoy methods. Furthermore it

also argued that the basis-efficiency mismatch can be removed entirely (for qubits received by Bob) if one randomly swaps the 0 and the 1 detector. Note that this trick, as argued in Ref. [13], *only works for the qubit subspace* and does not hold for higher photon numbers, which can be seen from our analysis in Section 6.4. Refs. [12, 33] extended this work without having to assume qubit detections, but still performs an asymptotic analysis. In Ref. [37], the numerical framework for key rate computations was proposed and used to compute IID asymptotic key rates for perfectly characterized and fixed basis-efficiency mismatch. In Ref. [14] the numerical framework [37] was used to compute IID asymptotic key rates for a toy model where Eve was allowed to induce basis efficiency mismatch via the use of two spatio-temporal modes. Recently, Ref. [15] improved upon [13] by obtaining tighter estimates on the phase error rate in the presence of basis efficiency mismatch, but again assumed IID collective attacks in the asymptotic regime, and single qubits received on Bob's side. The assumption of single qubits received by Bob was later removed in the follow up work [16]. In both [15, 16], Eve is not allowed to control the efficiency mismatch. A recent work [38] again considers a scenario with IID collective attacks in the asymptotic regime, but has the advantage of not requiring prior characterization of the detector parameters. Another recent work [34] combines qubit flaws in the source with efficiency mismatch in the detectors for coherent attacks, but is valid only in the asymptotic regime, and that Bob always receives a qubit. Finally, MDI-QKD [11] addresses *all* detector side-channels in the finite-size regime against coherent attacks, but requires a drastically different protocol implementation compared to standard QKD.

In comparison (as will fully see in the coming sections), this work:

1. **Does not assume IID collective attacks.**
2. **Is valid for finite-size settings.**
3. **Does not assume that Bob receives a qubit.**
4. **Requires no modifications or hardware changes to the protocol.**
5. **Also deals with dark counts.**
6. **Allows Eve to control the efficiency mismatch via spatio-temporal modes.**
7. **Can handle independent detectors (does not require IID detectors).**

2 Protocol Description

In this section we describe the steps of the QKD protocol we analyze.

1. **State Preparation:** Alice decides to send states in the basis Z (X) with probability $p^{(A)}_{(Z)}(p^{(A)}_{(X)})$. If she chooses the Z basis, she sends states $\{|0\rangle_{A'}, |1\rangle_{A'}\}$ with equal probability. If she chooses the X basis, she sends states $\{|+\rangle_{A'}, |-\rangle_{A'}\}$ with equal probability. She repeats this procedure n times. Notice that this ensures

$$\rho_{A'|X} = \frac{|+\rangle\langle+| + |-\rangle\langle-|}{2} = \frac{|0\rangle\langle0| + |1\rangle\langle1|}{2} = \rho_{A'|Z} = \frac{\mathrm{I}_{A'}}{2} \tag{1}$$

where $\rho_{A'|b}$ denotes the the state sent out from Alice's lab given that she chooses a basis b. Essentially, Eq. (1) says that the Alice's signal states leak no information about the basis chosen by Alice. This can be shown rigorously as follows.

Using the source-replacement scheme [39, 40], Alice's signal preparation is equivalent to her first preparing the state $|\Psi_+\rangle = \frac{|00\rangle_{AA'}+|11\rangle_{AA'}}{\sqrt{2}}$ followed by measurements on the A system. Eve is allowed to attack the A'^n system in any arbitrary (non-IID) manner, and forwards the system to B to Bob. Furthermore, without loss of generality, this process can be viewed as Alice *first* sending the system A' to Bob and *then* measuring her system.

Now, if Alice prepares the states from Eq. (1), her POVM elements corresponding to the basis b signal states sum to $p^{(A)}_{(b)}\mathrm{I}_A$. Because of this fact, one can view Alice's measurement

process, *after* using the source-replacement scheme, as equivalent to choosing the basis $Z(X)$ with probability $p_{(Z)}^{(A)}(p_{(X)}^{(A)})$, followed by measuring using the POVM $\{\Gamma_{(b,0)}^{(A)}, \Gamma_{(b,1)}^{(A)}\}$, for a given basis b. This reflects the fact that Eve has no knowledge of the basis used.

The POVM elements are given by

$$\begin{aligned} \Gamma_{(Z,0)}^{(A)} &= |0\rangle\langle 0|\,, \quad \Gamma_{(Z,1)}^{(A)} = |1\rangle\langle 1| \\ \Gamma_{(X,0)}^{(A)} &= |+\rangle\langle +|\,, \quad \Gamma_{(X,1)}^{(A)} = |-\rangle\langle -|\,. \end{aligned} \tag{2}$$

Therefore, we now have a setup where the state $\rho_{A^nB^n}$ is shared between Alice and Bob, followed by basis choice and measurements by Alice.

Remark 1. Without loss of generality, one can always use the source-replacement scheme, and delay Alice's measurements until after Eve's attack has been completed, for any set of signal states. However, this process might result in POVM elements for Alice whose sum (for a specific basis) is not proportional to identity. In this case, Alice's measurements are *incompatible with active basis choice* after the source-replacement scheme. We utilize the fact that Alice implements active basis choice when using the EUR statement (Section B), and in bounding the phase error rate (Sections 3 and 4). It is precisely for this reason that Eq. (1) is needed. For methods to address imperfect state preparation, we refer the reader to [7–10] (however we note that the analysis there is within the phase error framework).

2. **Measurement:** Bob chooses to measure in the $Z(X)$ basis with probability $p_{(Z)}^{(B)}(p_{(X)}^{(B)})$. For each basis choice, Bob has two threshhold detectors, each of which can click or not-click. Bob maps double clicks to 0/1 randomly (this is essential, see Remark 2), and thus has 3 POVM elements in each basis b, which we denote using $\{\Gamma_{(b,\perp)}^{(B)}, \Gamma_{(b,0)}^{(B)}, \Gamma_{(b,1)}^{(B)}\}$ which correspond to the inconclusive-outcome, 0-outcome, and the 1-outcome. In this work, we will use the following notation to write joint POVM elements,

$$\begin{aligned} \Gamma_{(b_A,b_B),(i,j)} &\coloneqq \Gamma_{(b_A,i)}^{(A)} \otimes \Gamma_{(b_B,j)}^{(B)}, \\ \Gamma_{(b_A,b_B),(\neq)} &\coloneqq \Gamma_{(b_A,0)}^{(A)} \otimes \Gamma_{(b_B,1)}^{(B)} + \Gamma_{(b_A,1)}^{(A)} \otimes \Gamma_{(b_B,0)}^{(B)}, \\ \Gamma_{(b_A,b_B),(=)} &\coloneqq \Gamma_{(b_A,0)}^{(A)} \otimes \Gamma_{(b_B,0)}^{(B)} + \Gamma_{(b_A,1)}^{(A)} \otimes \Gamma_{(b_B,1)}^{(B)}, \\ \Gamma_{(b_A,b_B),(\perp)} &\coloneqq \mathrm{I}_A \otimes \Gamma_{(b_B,\perp)}^{(B)}, \end{aligned} \tag{3}$$

where Alice's POVMs are defined in Eq. (2), and Bob's in Section 6.3.

Remark 2. As we will see in Section 3, the mathematical assumption on Bob's detector setup needed for phase error estimation is actually given by

$$\Gamma_{(X,\perp)}^{(B)} = \Gamma_{(Z,\perp)}^{(B)}. \tag{4}$$

This means that the probability of a round being inconclusive (i.e discarded) is independent of the basis for all input states. Notice that Eq. (4) depends on the choice of classical post-processing on Bob's side. In particular, it can be trivially satisfied by mapping no-click and double-click events to 0 and 1 randomly (so that $\Gamma_{(X,\perp)}^{(B)} = \Gamma_{(Z,\perp)}^{(B)}$ is zero). However, such a protocol cannot produce a key when loss is greater than 50%, and is therefore impractical. In general, if one assumes the canonical model of detectors (see Section 6.3), and maps double-clicks to 0/1 randomly, then Eq. (4) requires the loss and dark count rates in each detector-arm to be equal. This is why this condition is referred to as "basis-independent loss", and its violation is referred to as "detection-efficiency mismatch" in the literature. Note that even for identical detectors, one is forced remap double-click events to satisfy Eq. (4).

3. **Classical Announcements and Sifting:** For all rounds, Alice and Bob announce the basis they used. Furthermore, Bob announces whether he got a conclusive outcome ($\{\Gamma_{(b,0)}^{(B)}, \Gamma_{(b,1)}^{(B)}\}$), or

inconclusive ($\{\Gamma^{(B)}_{(b,\perp)}\}$). A round is said to be "conclusive" if Alice and Bob used the same basis, and Bob obtained a conclusive outcome.

On all the X basis conclusive rounds, Alice and Bob announce their measurement outcomes. These rounds are used to estimate the phase error rate. We let n_X be the number of X basis conclusive rounds, and let e_X^{obs} be the observed error rate in these rounds.

On all Z basis conclusive round, Alice and Bob announce their measurement outcomes with some small probability $p_{\text{Z,T}}$. We let e_Z^{obs} denote the observed error rate in these rounds, which is used to determine the amount of error-correction that needs to be performed. Note that this estimation need not be accurate for the purposes of proving security of the protocol. The remaining n_K rounds are used for key generation.

All these classical announcements are stored in the register C^n. The state of the protocol at this stage is given by $\rho_{Z_A^{n_K} Z_B^{n_K} C^n E^n | \Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}}$, where Z_A and Z_B denote Alice and Bob's raw key register, and $\Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}$ denotes the event that $n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}$ values are observed in the protocol.

Remark 3. In this work, we use bold letters, such as $\boldsymbol{x}$ to denote a classical random variable, and x to denote a particular value it takes. Furthermore, we will use $\Omega_{(x)}$ to denote the event that $\boldsymbol{x} = x$. Thus our protocol involves random variables $\boldsymbol{n_X}, \boldsymbol{n_K}, \boldsymbol{e_X^{\text{obs}}}, \boldsymbol{e_X^{\text{key}}}$, which take values $n_X, n_K, e_X^{\text{obs}}, e_X^{\text{key}}$ in any given run.

4. **Variable-Length Decision:** When event $\Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}$ occurs, Alice and Bob compute $\lambda_{\text{EC}}(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ (the number of bits to be used for one-way error-correction) and $l(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ (the length of the final key to be produced). Aborting is modeled as producing a key of length zero.

   Remark 4. Note that current security proofs do not allow users to *first* implement error-correction and *then* take the number of bits actually used as λ_{EC} in the security analysis. This is because the length of the error-correction string actually used in the protocol run leaks information about Alice and Bob's raw key data. This is because Eve can simulate the same error-correction protocol on all possible classical strings to determine which strings are compatible with the length she observes. This leakage is difficult to incorporate in security proofs.

   The variable-length protocol we consider allows users to determine the length of the error-correction information as a function of observations on the announced data. This data is anyway known to Eve, and therefore this procedure does not leak information via the above mechanism. Thus in this work, one must fix $\lambda_{\text{EC}}(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ to be a suitable function that determines the exact number of bits to be used for one-way error-correction, as a function of announcements. For more discussion, see footnote. [2].

5. **Error-correction and error-verification:** Alice and Bob implement error-correction using a one-way error-correction protocol with $\lambda_{\text{EC}}(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ bits of information. They implement error-verification by implementing a common two-universal hash function to $\log(2/\varepsilon_{\text{EV}})$ bits, and comparing the hash values. We let C_E be the classical register storing this communication, and note that it involves $\lambda_{\text{EC}}(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) + \log(2/\varepsilon_{\text{EV}})$ bits of communication (see footnote. [3]). We let Ω_{EV} denote the event that error-verification passes.

[2] In general, the number of bits leaked during error-correction is equal to the length of the classical bit string needed to encode all possible transcripts of the error-correction protocol (which can be one-way or two-way). Thus, if one requires $\lambda_{\text{EC}}(...)$ to be an upper bound on the number of bits used, then we can proceed by noting that the number of bit strings of length up to some value λ_{EC} is $2^{\lambda_{\text{EC}}+1} - 1$, so a $(\lambda_{\text{EC}} + 1)$-bit register suffices to encode all such bit strings. With this, it suffices to replace the $\lambda_{\text{EC}}(...)$ values in our subsequent key length formulas with $\lambda_{\text{EC}}(...) + 1$. A similar analysis can be done for other error-correction protocols as well.

[3] Technically, one also has to include the choice of the hash function and one bit for the result of the hash comparison. However, the choice of the hash function is independent of the QKD protocol, and thus gives no info to Eve. Moreover, the protocol aborts when hash comparison fails, and thus this extra bit takes a deterministic values and does not affect any entropies.

6. **Privacy Amplification:** Alice and Bob implement a common two-universal hash function (communicated using the register C_P), and produce a key of length $l(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$. The state of the protocol at this stage is given by $\rho_{K_A K_B C^n C_E C_P E^n | \Omega(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) \wedge \Omega_{\text{EV}}}$.

Notice here that we implement a variable-length protocol. Such protocols are advantageous to fixed-length protocols, since they do not require Alice and Bob to properly characterize their channel before runtime, and carefully choose the acceptance critera. Instead, they can adjust the length of the key produced to the appropriate length, depending on the observed values during runtime. For the above protocol, the variable-length decision is a function of $n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}$.

2.1 Requirements on phase error estimation procedure and variable-length security

We now turn our attention to the estimation of the phase error rate. Note that in a QKD protocol, one starts with a fixed but unknown state $\rho_{A^n B^n E^n}$ that represents Eve's attack. This state then gives rise to random variables $\boldsymbol{n_X}, \boldsymbol{n_K}, \boldsymbol{e_X^{\text{obs}}}, \boldsymbol{e_X^{\text{key}}}$. Here $\boldsymbol{e_X^{\text{key}}}$ denotes the random variable corresponding to the "phase error rate" in the key-generation rounds, when Alice and Bob measure those rounds (virtually) in the X basis. (The phase error rate is explained in greater detail in Sections 3 and 4). To obtain variable-length security, one must obtain a high probability upper bound on the phase error rate $\boldsymbol{e_X^{\text{key}}}$. We assume that one has a way to obtain the following statement (which we prove in Sections 3 and 4):

$$\Pr\left(\boldsymbol{e_X^{\text{key}}} \geq \mathcal{B}_{\delta_1,\delta_2}(\boldsymbol{e_X^{\text{obs}}}, \boldsymbol{n_X}, \boldsymbol{n_K})\right) \leq \varepsilon_{\text{AT}}^2. \tag{5}$$

This states that the phase error rate is upper bounded (with high probability) by a suitable function $\mathcal{B}_{\delta_1,\delta_2}$ of the observed error rate in the X basis rounds, and the number of test and key generation rounds. We will obtain a suitable $\mathcal{B}_{\delta_1,\delta_2}$ satisfying Eq. (5) in Sections 3 and 4, with and without the basis-independent loss assumption. The function $\mathcal{B}_{\delta_1,\delta_2}$ depends on the metrics δ_1, δ_2 that quantify the deviation from ideal behavior for a given protocol description. We compute explicit bounds for δ_1, δ_2 for detectors with efficiency mismatch in Section 6.4 using the recipe outlined in Section 6.1.

Remark 5. When working with random variables that are obtained via measurements on quantum states, the joint distributions of random variables can only be specified when those random variables *can exist at the same time*, via some physical measurements on the state. For example, one cannot speak of the joint distribution of X and Z measurement outcomes on the *same* state, since such a joint distribution does not exist. In the entirety of this work, all the random variables whose joint distribution is used in our arguments can indeed exist at the same time.

Given an upper bound on the phase error rate (Eq. (5)), we have the following theorem regarding the variable-length security of the QKD protocol described above. The proof is essentially identical to [32, Supplementary Note A], and uses the same techniques as those in Refs. [30, 31] and is included in Section B.

Theorem 1. [Variable-length security of BB84 with qubit source] Suppose Eq. (5) is satisfied and let $\lambda_{\text{EC}}(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ be a function that determines the number of bits used for error-correction. Define

$$\begin{aligned} l(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) \coloneqq \max\Big(0, n_K\left(1 - h\left(\mathcal{B}_{\delta_1,\delta_2}(e_X^{\text{obs}}, n_X, n_K)\right)\right) - \lambda_{\text{EC}}(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) \\ - 2\log(1/2\varepsilon_{\text{PA}}) - \log(2/\varepsilon_{\text{EV}})\Big), \end{aligned} \tag{6}$$

where $h(x)$ is the binary entropy function for $x \leq 1/2$, and $h(x) = 1$ otherwise. Then the variable-length QKD protocol that produces a key of length $l(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ using $\lambda_{\text{EC}}(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ bits for error-correction, upon the event $\Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})} \wedge \Omega_{\text{EV}}$ is $(2\varepsilon_{\text{AT}} + \varepsilon_{\text{PA}} + \varepsilon_{\text{EV}})$-secure [4].

[4] For pedagogical reasons, we ignore the issues arising from non-integer values of hash-lengths. Such issues can be easily fixed by suitable use of floor and ceiling functions.

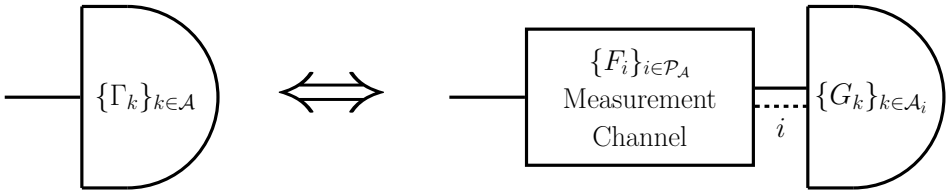


Figure 1: Schematic for the two-step measurement procedure from Lemma 1. Note that the second step measurement $\{G_k\}_{k\in\mathcal{A}_i}$ depends on the outcome of the first step measurement.

3 Phase error estimation with basis-independent loss assumption

In this section, we will prove Eq. (5) for an implementation that satisfies the basis-independent loss assumption. It is useful to refer to Fig. 2 for this section. To prove Eq. (5), we will need to modify the actual protocol to an equivalent protocol (in the sense of being the same quantum to classical channel). To do so we will use Lemma 1 below to reformulate Alice and Bob's measurements to consist of two steps. The first step will implement a basis-*independent* filtering operation that discards the inconclusive outcomes, while the second step will complete the measurement procedure. Then the required claim will follow from random sampling arguments on the second step measurements. We start by explaining the two-step protocol measurements.

3.1 Protocol Measurements

We will first use the following lemma to divide Alice and Bob's measurement procedure into two steps. For the proof, we refer the reader to Section A. We will use $S_\bullet(A)$ and $S_\circ(A)$ to denote the set of sub-normalized and normalized states on the register A respectively.

Lemma 1. [Filtering POVMs] Let $\{\Gamma_k | k \in \mathcal{A}\}$ be a POVM on a register Q, and let $\{\mathcal{A}_i\}_{i\in\mathcal{P}_\mathcal{A}}$ be a partition of $\mathcal{A}$, and let $\rho \in S_\bullet(Q)$ be a state. The classical register storing the measurement outcomes when ρ is measured using $\{\Gamma_k\}_{k\in\mathcal{A}}$ is given by

$$\rho_{\text{final}} \coloneqq \sum_{k\in\mathcal{A}} \operatorname{Tr}(\Gamma_k \rho) \, |k\rangle\langle k| \, . \tag{7}$$

This measurement procedure is equivalent (in the sense of being the same quantum to classical channel) to the following two-step measurement procedure: First doing a coarse-grained "filtering" measurement of i, using POVM $\{\tilde{F}_i\}_{i\in\mathcal{P}_\mathcal{A}}$, where

$$\begin{aligned} \tilde{F}_i &\coloneqq \sum_{j\in\mathcal{A}_i} \Gamma_j, \qquad \text{leading to the post-measurement state} \\ \rho'_{\text{intermediate}} &= \sum_{i\in\mathcal{P}_\mathcal{A}} \sqrt{\tilde{F}_i}\rho\sqrt{\tilde{F}_i}^\dagger \otimes |i\rangle\langle i| \, . \end{aligned} \tag{8}$$

Upon obtaining outcome i in the first step, measuring using POVM $\{G_k\}_{k\in\mathcal{A}_i}$ where

$$\begin{aligned} G_k &\coloneqq \sqrt{\tilde{F}_i}^+ \Gamma_k \sqrt{\tilde{F}_i}^+ + P_k \qquad \text{leading to the post-measurement classical state} \\ \rho'_{\text{final}} &= \sum_{i\in\mathcal{P}_\mathcal{A}} \sum_{k\in\mathcal{A}_i} \operatorname{Tr}\left(G_k \sqrt{\tilde{F}_i}\rho\sqrt{\tilde{F}_i} \right) |k\rangle\langle k| \, , \end{aligned} \tag{9}$$

where F^+ denotes the pseudo-inverse of F, and P_k are any positive operators satisfying $\sum_{k\in\mathcal{A}_i} P_k = \mathrm{I} - \Pi_{\tilde{F}_i}$, where $\Pi_{\tilde{F}_i}$ denotes the projector onto the support of $\tilde{F}_i$.

Consider the POVMs $\{\Gamma_{(b_A,b_B),(\neq)}, \Gamma_{(b_A,b_B),(=)}, \Gamma_{(b_A,b_B),(\perp)}\}$ defined in Eq. (3), which correspond to Bob obtaining a conclusive outcome and Alice and Bob obtaining an error, Bob obtaining a conclusive outcome and Alice and Bob not obtaining an error, and Bob obtaining an inconclusive outcome respectively, for basis choices b_A, b_B. Without loss of generality, we can use Lemma 1 to equivalently describe Alice and Bob's measurement procedure as consisting of two steps.

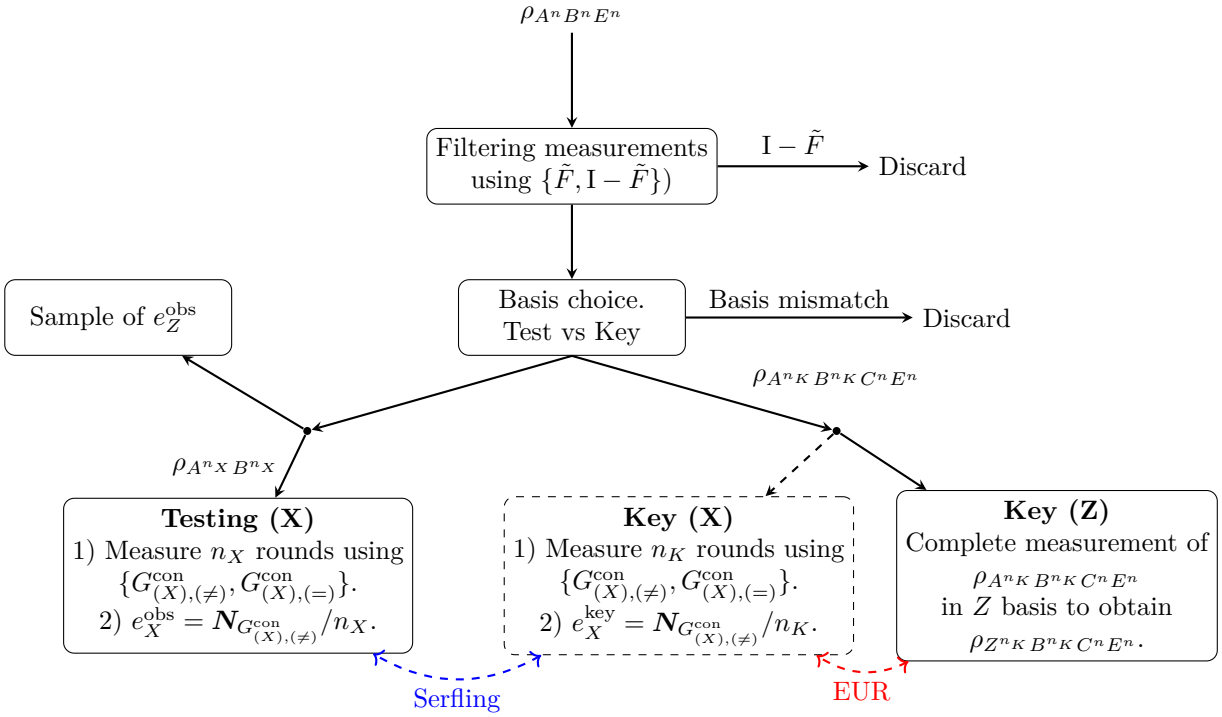


Figure 2: Protocol flowchart for the equivalent protocol from Section 3, where basis-independent loss assumption (Eq. (4)) is satisfied. The dotted arrows and boxes represent virtual measurements that do not actually happen in the real protocol. Connections between different boxes are highlighted using curved arrows. We use the Serfling bound (Lemma 2) to obtain a bound on the phase error rate from observations. The phase error rate is then used to bound the smooth min entropy using the EUR statement. We use $\boldsymbol{N}_P$ to denote the number of P measurement outcomes, where P denotes a POVM element. For clarity, we have omitted the conditioning on events in the figure (but not in our proof). The basis used for measurements is indicated in each box, and refers to the basis used by *both* Alice and Bob.

1. First, they measure using POVM $\{\tilde{F}_{(b_A,b_B),(\mathrm{con})}, \tilde{F}_{(b_A,b_B),(\perp)}\}$ which determines whether they obtain a conclusive and inconclusive measurement outcome.

2. Then, if they obtain a conclusive outcome, they measure using a second POVM $\{G^{\mathrm{con}}_{(b_A,b_B),(=)}, G^{\mathrm{con}}_{(b_A,b_B),(\neq)}\}$.

We use the convention that whenever an explicit basis (X/Z) is written in the subscript of these POVMs, it refers to the basis used by both Alice and Bob. We refer to the first-step measurements as "filtering" measurements, since they determine whether Bob gets a conclusive outcome (which may be kept or discarded depending on basis choice), or an inconclusive outcome (which is always discarded). Furthermore, due to the construction of the POVM from Lemma 1, we have

$$\tilde{F}_{(b_A,b_B),(\perp)} = \mathrm{I}_A \otimes \Gamma^{(B)}_{(b_B,\perp)}. \tag{10}$$

3.2 Constructing an equivalent protocol

We will now construct an equivalent protocol that is described in Fig. 2.

1. If one has $\Gamma^{(B)}_{(X,\perp)} = \Gamma^{(B)}_{(Z,\perp)}$, then we find that the filtering measurements $\tilde{F}_{(b_A,b_B),(\mathrm{con})}$ is independent of the basis choices (b_A, b_B). Let this basis-independent POVM element be $\tilde{F}$. If the filtering measurement does not depend on the basis choice, then implementing the basis choice followed by filtering measurement is the same as implementing the filtering measurement followed by basis choice. Thus, we can delay basis choice until after the filtering measurements have been performed. This can also be formally argued using Lemma 1. This allows us to obtain the first node of Fig. 2, where we measure using $\{\tilde{F}, \mathrm{I} - \tilde{F}\}$.

2. This is then followed by random basis choices and assignment to test vs key by Alice and Bob. All X basis rounds are used for testing, while most Z basis rounds are used for key generation (and a small fraction is used to estimate e_Z^{obs}). Thus, we get the second node of Fig. 2. Note that the estimate e_Z^{obs} of the error rate in the key bits is only used to determine the amount of error-correction required and does not affect the secrecy of the protocol. However, e_Z^{obs} and the choice of error-correction protocol is important to ensure that error-verification succeeds with high probability.

3. The n_X testing rounds are measured using $\{G^{\text{con}}_{(X),(=)}, G^{\text{con}}_{(X),(\neq)}\}$, and the error rate in these rounds is denoted by e_X^{obs}. This is the error rate we observe. This is the **Testing (X)** node of Fig. 2.

4. The n_K key generation rounds can be measured (virtually) using the same POVM $\{G^{\text{con}}_{(X),(=)}, G^{\text{con}}_{(X),(\neq)}\}$. The error rate in these rounds is denoted by e_X^{key} and is the phase error rate we wish to estimate. This is the **Key (X)** node of Fig. 2.

5. The actual n_K key generation rounds are measured in the Z basis to obtain the raw key. This is the **Key (Z)** node of Fig. 2.

3.3 Sampling

We will now turn our attention to the sampling part of the argument, and obtain an estimate $\mathcal{B}_{0,0}$ on the phase error rate that satisfies Eq. (5). To do so, we will make use of the following Lemma, which uses the Serfling bound [41]. For the proof, we refer the reader to Section C.1.

Lemma 2. [Serfling with IID sampling] Let $\boldsymbol{X}_1 \dots \boldsymbol{X}_n$ be bit-valued random variables. Suppose each position i is mapped to the "test set" ($i \in \boldsymbol{J}_t$) with probability p_t, and the "key set" ($i \in \boldsymbol{J}_k$) with probability p_k. Let $\Omega_{(n_X,n_K)}$ be the event that exactly n_X positions are mapped to test, and exactly n_K positions are mapped to key. Then, conditioned on the event $\Omega_{(n_X,n_K)}$, the following statement is true:

$$\Pr\left(\sum_{i\in\boldsymbol{J}_k}\frac{\boldsymbol{X}_i}{n_K} \geq \sum_{i\in\boldsymbol{J}_t}\frac{\boldsymbol{X}_i}{n_X} + \gamma_{\text{serf}}\right)_{|\Omega_{(n_X,n_K)}} \leq e^{-2\gamma_{\text{serf}}^2 f_{\text{serf}}(n_X,n_K)}, \tag{11}$$

$$f_{\text{serf}}(n_X,n_K) \coloneqq \frac{n_K n_X^2}{(n_K+n_X)(n_X+1)}.$$

To use the lemma, we will identify $X_i = 1$ with error, and $X_i = 0$ with the no-error outcome, when the conclusive rounds are measured in the X basis. The test data will correspond to e_X^{obs}, whereas the key data will correspond to e_X^{key}.

Remark 6. There are two important aspects to the sampling argument. First, the Serfling bound applies in the situation where one chooses a random subset of *fixed-length* for testing. However, the above procedure (and many QKD protocols) randomly assigns each round to testing vs key generation. Thus, Serfling must be applied with some care, and that is what is done here (see footnote. [5]). This observation has been missing in many prior works. Second, since we are interested in a variable-length protocol, we require slightly different statements than standard fixed-length security proofs (Eq. (5)). However, these can also be obtained by simple (almost trivial) modifications to existing arguments and yield the same results as before. Both these issues are addressed in the proof of Lemma 2 in Section C.

Let us consider the second node in the equivalent protocol constructed in Fig. 2, where rounds are now randomly assigned for testing (X basis) or key generation (Z basis and key generation). (The remaining rounds are used for estimating the Z basis error rate or discarded and are unimportant for this discussion). Consider the state $\rho_{|\Omega_{(n_X,n_K)}}$, where the number of rounds to be used

[5] It is also worthwhile to note that if one is interested in estimating the QBER *independent* of basis, then the standard serfling argument is directly applicable (for instance in [2]).

to testing and key generation is fixed. Using Lemma 2 on this state, we obtain

$$\Pr\left(\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}} \geq \boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}} + \gamma_{\text{serf}}\right)_{|\Omega_{(n_X,n_K)}} \leq e^{-2\gamma_{\text{serf}}^2 f_{\text{serf}}(n_X,n_K)}, \tag{12}$$

Furthermore we can choose

$$\gamma_{\text{serf}}^{\varepsilon_{\text{AT}}}(n_X,n_K) \coloneqq \sqrt{\frac{\ln(1/\varepsilon_{\text{AT}}^2)}{2f_{\text{serf}}(n_X,n_K)}} \implies e^{-2\left(\gamma_{\text{serf}}^{\varepsilon_{\text{AT}}}(n_X,n_K)\right)^2 f_{\text{serf}}(n_X,n_K)} = \varepsilon_{\text{AT}}^2. \tag{13}$$

Thus we can choose

$$\mathcal{B}_{0,0}(e_X^{\text{obs}}, n_X, n_K) = e_X^{\text{obs}} + \gamma_{\text{serf}}^{\varepsilon_{\text{AT}}}(n_X,n_K) \tag{14}$$

to be our bound for the phase error rate, where the $(0,0)$ subscript indicates that the bound is only valid when there is no deviation from basis-independent loss. Finally, since the bound is valid for any event $\Omega(n_X,n_K)$, we can get rid of this conditioning in Eq. (12), to obtain Eq. (5) via

$$\begin{aligned}\Pr\left(\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}} \geq \mathcal{B}_{0,0}(\boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}}, \boldsymbol{n_X}, \boldsymbol{n_K})\right) &= \sum_{n_X,n_K} \Pr\left(\Omega_{(n_X,n_K)}\right) \Pr\left(\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}} \geq \mathcal{B}_{0,0}(\boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}}, n_X, n_K)\right)_{|\Omega_{(n_X,n_K)}} \\ &\leq \sum_{n_X,n_K} \Pr\left(\Omega_{(n_X,n_K)}\right) \varepsilon_{\text{AT}}^2 \\ &= \varepsilon_{\text{AT}}^2\end{aligned} \tag{15}$$

(In this work, we will use the convention that $\sum_x$ denotes the sum over all possible values x can take). Thus, for the above choice of $\mathcal{B}_{0,0}(e_X^{\text{obs}}, n_X, n_K)$, the variable-length security of the protocol follows from Theorem 1.

4 Phase error estimation without basis-independent loss assumption

In this section, we will prove Eq. (5) for an implementation that *does not satisfy* the basis-independent loss assumption. The argument is similar to the one presented in Section 3, with important additions. It is helpful to refer to Fig. 3 for this section. We will first explain the idea behind the proof, before stating the proof itself.

Proof Idea

We will use Lemma 1 in Section 4.1 to construct an equivalent measurement procedure (in the sense that it is the same quantum to classical channel) for the protocol, which consists of three steps. The first step measurement is done using the POVM $\{\tilde{F}, \mathrm{I} - \tilde{F}\}$ and implements basis-*independent* filtering (discarding) operations. ($\tilde{F}$ here plays the same role as in Section 3, but is defined differently). In particular it is the largest common filtering operation over both basis choices.

Due to basis-efficiency mismatch, we will have a second step measurement that implements filtering operations that depends on the basis choice. (This will typically result in a small number of discards for a small amount of basis-dependent loss in the detectors). Once both filtering steps are done, the measurements on the remaining rounds can be completed using the third step measurements which determines the exact measurement outcomes on the detected rounds.

Turning our attention to Fig. 3, the state first undergoes the basis-independent filtering measurement in the first node. This is then followed by random basis choice and assignment to testing and key generation at the second node. The testing rounds are further measured using second step X basis filtering POVM and third step X basis POVM at the **Testing*** $(X \to X)$ node. Similarly, the key generation rounds are measured using second step Z basis filtering POVM and third step Z basis POVM. Note that we use $(b_{\text{2nd}} \to b_{\text{3rd}})$ to denote the basis choice b_{2nd} for the second step filtering measurement, and basis choice b_{3rd} for the third step measurement, for both Alice and Bob.

We will consider virtual measurements on the key generation rounds corresponding to $X \to X$ and $Z \to X$. These are represented using dotted boxes and lines in the figure. These measurements

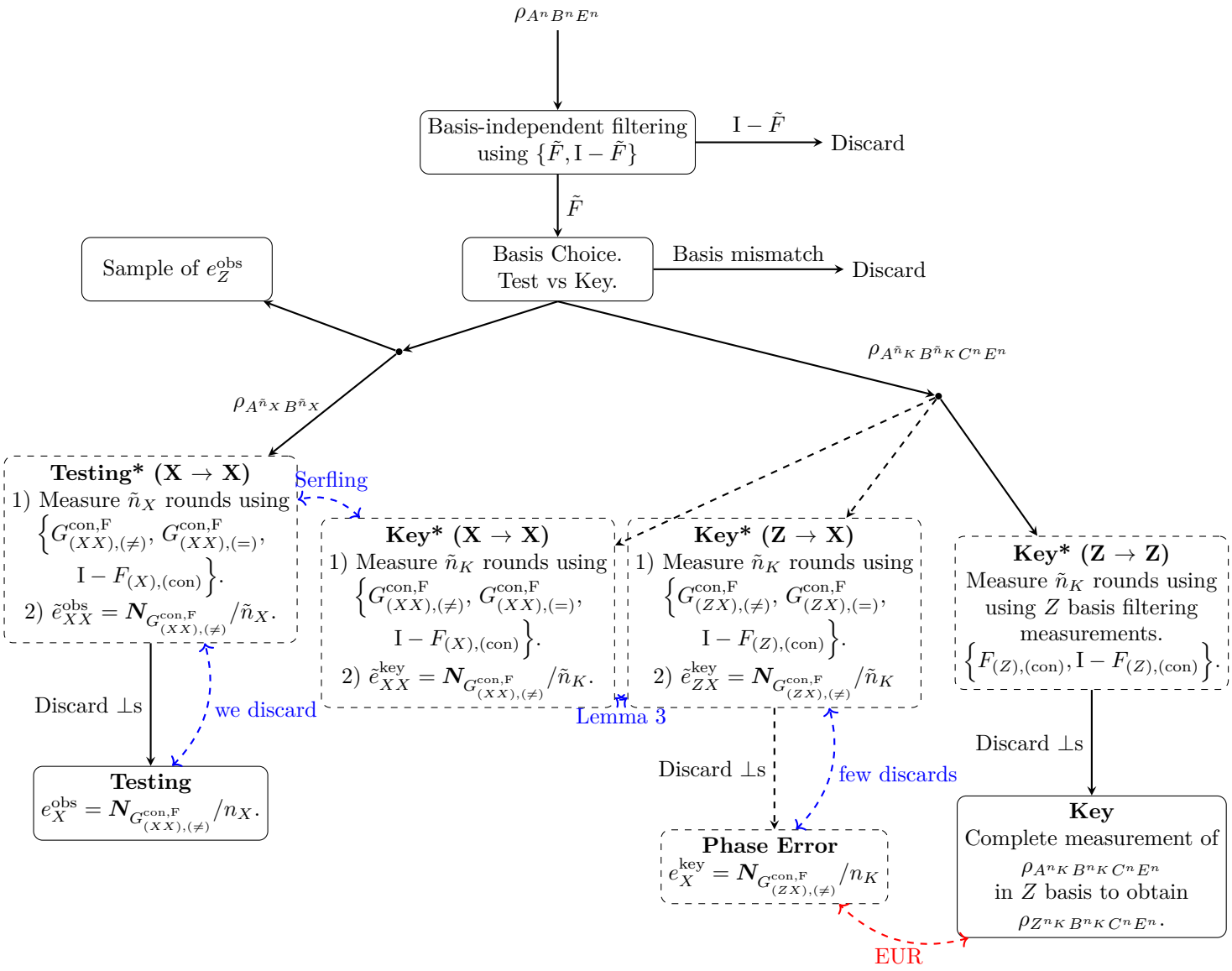


Figure 3: Protocol flowchart for the equivalent protocol from Section 4, where basis-independent loss assumption (Eq. (4)) is not satisfied. The dotted arrows and boxes represent virtual measurements that do not actually happen in the real protocol. Connections between the error rates in different boxes are highlighted using curved arrows. We use $\boldsymbol{N}_P$ to denote the number of P measurement outcomes, where P denotes a POVM element. For the POVMs, the reader may refer to Table 2 or Section 4.1. For clarity, we have omitted the conditioning on events in the figure (but not in our proof). Compared to Fig. 3, the testing and key generation rounds go through an additional second step filtering measurement that depends on the basis used, which typically results in a few rounds being discarded, before undergoing the final measurement. The basis used in these measurements in indicated in each box, and indicates the basis used by *both* Alice and Bob.

are not performed in the protocol, but are only required in our proof. We will then associate an error rate with all these choices of measurements, which corresponds to the number of rounds that resulted in an error divided by the total number of rounds on which the measurements were done.

We see a variety of error rates in Fig. 3. These errors are classified based on three criteria: 1) The basis used by Alice *and* Bob in the second and third step measurements (written in the subscript), 2) Whether the $\perp$s due to the second step measurements have been discarded from the total number of rounds or not (e vs $\tilde{e}$), 3) Whether they were done on testing rounds (obs in superscript), or key generation rounds (key in superscript). The proof will follow by building a connection from our observed error rate (e_X^{obs}), to the phase error rate (e_X^{key}). These connections are highlighted using curved blue arrows in the figure. Note that we only observe the error rate e_X^{obs} in the protocol.

In particular, we will relate the error rates before and after discarding for the testing rounds ($\tilde{e}_{XX}^{\text{obs}} \leftrightarrow e_X^{\text{obs}}$) by simply noting that we discard rounds in the second-step measurements. On the other hand, we will relate $\tilde{e}_{ZX}^{\text{key}} \leftrightarrow e_X^{\text{key}}$ by bounding the number of discards that can happen in the second step filtering measurements. This relation will depend on δ_2, which will be the metric that quantifies the "smallness" of the POVM element corresponding to the discard outcome. $\tilde{e}_{XX}^{\text{obs}}$ and $\tilde{e}_{XX}^{\text{key}}$ correspond to error rates corresponding to exactly the same measurement, and assigned to test vs key randomly. Thus, they can be related using Serfling (Lemma 2), exactly as in Section 3. $\tilde{e}_{XX}^{\text{key}}$ and $\tilde{e}_{ZX}^{\text{key}}$ correspond to error rates on the same state, but with slightly different POVMs, and thus are expected to be similar. This can be rigorously argued using Lemma 3, where we use δ_1 to quantify the "closeness" of these POVMs. Combining all these relations, we will ultimately obtain Eq. (34).

We will now convert the above sketch into a rigorous proof. We start by explaining the three step protocol measurements.

4.1 Protocol Measurements

Fix the basis b_A, b_B used by Alice and Bob. As in Section 3.1, consider the POVM $\{\Gamma_{(b_A,b_B),(\neq)}, \Gamma_{(b_A,b_B),(=)}, \Gamma_{(b_A,b_B),(\perp)}\}$ defined in Eq. (3), which correspond to Bob obtaining a conclusive outcome (and Alice and Bob obtaining an error), Bob obtaining a conclusive outcome (and Alice and Bob not obtaining an error), and Bob obtaining an inconclusive outcome respectively. Since $\Gamma_{(b_A,b_B),(\perp)}$ now depends on the basis choices, we cannot proceed in the same way as before. This reflects the fact that the discarding is basis dependent. Thus we will reformulate the measurement process in a different way.

To do so, consider a $\tilde{F}$ such that

$$\tilde{F} \geq \Gamma_{(b_A,b_B),(=)} + \Gamma_{(b_A,b_B),(\neq)} \quad \forall (b_A, b_B) \tag{16}$$

This $\tilde{F}$ will play the role of a common "basis-independent filtering measurement". While any choice satisfying the above requirement will suffice, for the best results, $\tilde{F}$ must fulfil Eq. (16) as tightly as possible.

Remark 7. Since basis-mismatch rounds are discarded anyway, it is possible to argue that we only need $\tilde{F}$ to satisfy $\Gamma_{(b_A,b_B),(=)} + \Gamma_{(b_A,b_B),(\neq)} \leq \tilde{F}$ for $b_A = b_B$. This involves constructing a slightly different equivalent protocol where the first node decides basis match vs mismatch. The basis match events then undergo the usual filtering followed by basis choice, while the mismatch events are discarded without any filtering. If this modified requirement results in a value of $\tilde{F}$ that is "smaller" then the original choice, then this will lead to tighter key rates. Intuitively, this is due to the fact that a smaller value of $\tilde{F}$ means that more loss is attributed to the basis-independent filtering.

To reformulate the measurement procedure, start by considering the four-outcome POVM given by $\{\mathrm{I} - \tilde{F}, \tilde{F} - \Gamma_{(b_A,b_B),(=)} - \Gamma_{(b_A,b_B),(\neq)}, \Gamma_{(b_A,b_B),(=)}, \Gamma_{(b_A,b_B),(\neq)}\}$, where the first two outcomes correspond to discard, the third correspond to a conclusive no-error outcome, and the fourth corresponds to a conclusive error. This four-outcome measurement followed by classical grouping of the first two outcomes is then equivalent to the original three-outcome measurement in the protocol.

Now, we can use Lemma 1 to reformulate the four-outcome measurement as occurring in two steps. In the first step, Alice and Bob measure using POVM $\{\tilde{F}, \mathrm{I} - \tilde{F}\}$ and discard the latter outcomes. If they obtain the $\tilde{F}$ outcome, they then complete the measurement using POVM $\{\tilde{F}_{(b_A,b_B),(\perp)}, \tilde{F}_{(b_A,b_B),(=)}, \tilde{F}_{(b_A,b_B),(\neq)}\}$, corresponding to discard, conclusive no-error and conclusive error outcomes respectively.

We then use Lemma 1 again to reformulate this three-outcome measurement to consist of two steps. First, they measure using $\{F_{(b_A,b_B),(\mathrm{con})}, F_{(b_A,b_B),(\perp)}\}$ which determines whether they obtain a conclusive or inconclusive measurement outcome. Then, if they obtain a conclusive outcome, they measure using the POVM $\{G^{\mathrm{con}}_{(b_A,b_B),(=)}, G^{\mathrm{con}}_{(b_A,b_B),(\neq)}\}$. Thus we now have a three-step measurement procedure, described in Table 2.

Since basis-mismatch signals are anyway discarded in the protocol, from this point onwards, we will only be concerned with POVMs that correspond to Alice and Bob choosing the same basis. As before, we will use the convention that whenever a basis is explicitly written as X/Z (or denoted using b_1b_2), it represents *both* Alice and Bob's basis choices.

It will be convenient to recombine the second and third step measurement into a single measurement step with three outcomes. For brevity we introduce the following notation to write this POVM $\{G^{\mathrm{con,F}}_{(b_1b_2),(\neq)}, G^{\mathrm{con,F}}_{(b_1b_2),(=)}, \mathrm{I} - F_{(b_1),(\mathrm{con})}\}$ where

$$\begin{aligned} G^{\mathrm{con,F}}_{(b_1b_2),(\neq)} &= \sqrt{F_{(b_1),(\mathrm{con})}}\, G^{\mathrm{con}}_{(b_2),(\neq)} \sqrt{F_{(b_1),(\mathrm{con})}}, \\ G^{\mathrm{con,F}}_{(b_1b_2),(=)} &= \sqrt{F_{(b_1),(\mathrm{con})}}\, G^{\mathrm{con}}_{(b_2),(=)} \sqrt{F_{(b_1),(\mathrm{con})}}. \end{aligned} \tag{17}$$

where the subscript b_1b_2 determines the basis for the second step and third step measurements by *both* Alice and Bob, and the superscript F indicates the merging of the two measurement steps. (Note that if $b_1 = b_2 = b$, then this simply reverses the earlier action of Lemma 1 that split $\{\tilde{F}_{(b,b),(\perp)}, \tilde{F}_{(b,b),(=)}, \tilde{F}_{(b,b),(\neq)}\}$ to generate the second and third-step measurements. However, we will consider fictitious measurements where $b_1 \neq b_2$ in our proof. To describe such measurements, it is indeed necessary to split $\{\tilde{F}_{(b_A,b_B),(\perp)}, \tilde{F}_{(b_A,b_B),(=)}, \tilde{F}_{(b_A,b_B),(\neq)}\}$ into two separate steps.)

Symbol	**Meaning**
$\{\tilde{F}, \mathrm{I} - \tilde{F}\}$	First step measurement. Implements basis-independent filter.
$\{F_{(b_A,b_B),(\mathrm{con})}, \mathrm{I} - F_{(b_A,b_B),(\mathrm{con})}\}$.	Second step measurement. Implements filtering that is basis dependent.
$\{G^{\mathrm{con}}_{(b_Ab_B),(=)}, G^{\mathrm{con}}_{(b_Ab_B),(\neq)}\}$	Third step measurement corresponding to no-error and error.
$\{G^{\mathrm{con,F}}_{(b_1b_2),(\neq)}$, $G^{\mathrm{con,F}}_{(b_1b_2),(=)}, \mathrm{I} - F_{(b_1),(\mathrm{con})}\}$	Combined second and third step measurement, corresponding to no-error, error and discard.
$\tilde{n}_X$	Number of testing rounds after basis-independent filter only
$\tilde{n}_K$	Number of key generation rounds after basis-independent filter only
n_X	Actual number of testing rounds
n_K	Actual number of key generation rounds

Table 2: Different symbols used in our proof. Note that b_A, b_B refer to basis choice of Alice and Bob. However, b_1, b_2 refer to the basis used by *both* Alice and Bob, for the second and third step measurements. Whenever a basis is explicitly written as X/Z (or b_1, b_2) it represents *both* Alice and Bob's basis choices.

4.2 Constructing an equivalent protocol

We will now construct the equivalent protocol from Fig. 3. The construction is similar to the one from Section 3.2, albeit with some important modifications.

1. As in Section 3.2, we observe that the first step measurement is conducted using $\{\tilde{F}, \mathrm{I} - \tilde{F}\}$ and is independent of basis. Therefore, we can delay basis choice until after this measurement has been completed, and the $\mathrm{I} - \tilde{F}$ outcomes are discarded. That is the first node of Fig. 3.

2. The remaining rounds undergo random basis choice. Basis mismatch rounds are discarded, all X basis rounds are used for testing, while Z basis rounds are probabilistically chosen for testing and key generation. This allows us to obtain the second node of Fig. 3. Again, as in Section 3.2, the estimate we obtain on e_Z^{obs} does not affect the secrecy claim of the protocol, since e_Z^{obs} is only used to determine the amount of error-correction to be performed.

Note that unlike Section 3.2, we have to perform *two* measurements on the testing and key generation rounds after the second node, and these rounds are *not* guaranteed to result in a conclusive outcome. We describe these measurements in detail below.

4.2.1 Testing Rounds after basis-independent Filter

We will now complete the measurement steps on the test rounds (which take place in the **Testing*** $(X \to X)$ box in Fig. 3). Let us consider the X basis rounds used for testing at this stage. Let $\tilde{n}_X$ be the number of such rounds. Note that some of these rounds will be discarded during the remainder of the protocol, and therefore we do not know the value of $\tilde{n}_X$ in the actual protocol. However, we will see that we do not need to.

These rounds must undergo the second step filtering measurement using $\{F_{(X),(\text{con})}, \mathrm{I}-F_{(X),(\text{con})}\}$, where the rounds which yield the latter outcome are discarded. Now, the remaining rounds are measured using the third step $\{G^{\text{con}}_{(X),(=)}, G^{\text{con}}_{(X),(\neq)}\}$ that determines whether Alice and Bob observe an error or no error. Recall that we use the convention that whenever a basis is explicitly written as X/Z, it refers to *both* Alice and Bob measuring in the same basis.

Combining the second and third measurement step, we see that measuring $\tilde{n}_X$ rounds using the above two-step procedure is equivalent to measuring directly using $\left\{G^{\text{con,F}}_{(XX),(\neq)}\ , G^{\text{con,F}}_{(XX),(=)}, \mathrm{I}-F_{(X),(\text{con})}\right\}$ (see Eq. (17)), with the outcomes corresponding conclusive and error, conclusive and no-error and inconclusive respectively. We write $\tilde{e}^{\text{obs}}_{XX}$ be the error rate in these rounds, which is the fraction of rounds that resulted in the $G^{\text{con,F}}_{(XX),(\neq)}$-outcome. The subscript XX reflects the fact that this is the error rate when the second step and third step measurements are in X basis. Note that we do not actually observe this error rate in the protocol. We write e^{obs}_X as the error rate in these rounds after discarding the $\perp$ outcomes. This is the error rate we actually observe in the protocol.

4.2.2 Key Generation Rounds after basis-independent Filter

We will now complete the virtual measurement steps on the key generation rounds, that lead to the phase error rate (which take place in the **Key*** $(Z \to X)$ box in Fig. 3). Let us consider the Z basis rounds selected for key generation at this stage. Let $\tilde{n}_K$ be the number of such rounds. Note that some of these rounds will be discarded during the remainder of the protocol, and therefore we do not actually know the value of $\tilde{n}_K$ in the protocol. However, as in the case of $\tilde{n}_X$, we do not need to.

These rounds must undergo the second step filtering measurement using $\{F_{(Z),(\text{con})}, \mathrm{I}-F_{(Z),(\text{con})}\}$, where the rounds which yield the latter outcome are discarded. Now, we wish to obtain the phase error rate when the remaining rounds are measured using the third step $\{G^{\text{con}}_{(X),(\neq)}, G^{\text{con}}_{(X),(=)}\}$ that determines whether Alice and Bob observe an error or no error.

Again, the above two-step measurement procedure is equivalent to measuring directly using $\left\{G^{\text{con,F}}_{(ZX),(\neq)}, G^{\text{con,F}}_{(ZX),(=)}, \mathrm{I}-F_{(Z),(\text{con})}\right\}$ (see Eq. (17)), with the outcomes corresponding conclusive and error, conclusive and no-error and inconclusive respectively. We let $\tilde{e}^{\text{key}}_{ZX}$ be the error rate in these rounds, which is the fraction of rounds that resulted in the $G^{\text{con,F}}_{(ZX),(\neq)}$-outcome. Again, the subscripts denote the fact that this is the error rate when the second step measurement is in the Z basis and the third step measurement is in the X basis. The phase error rate e^{key}_X is the error rate in these rounds after discarding the $\perp$ outcomes.

Remark 8. When basis-efficiency mismatch is present, one must figure out the phase error rate in the key generation rounds, which are filtered using the Z basis. However the rounds for testing are filtered using the X basis. These filtering steps are not identical. Therefore it becomes very difficult

to prove rigorous bounds on the phase error rate based on the observed data. One of the main contributions of this work is a rigorous derivation of such bounds, without relying on asymptotic behavior or IID assumptions.

Since the measurements in the key generation rounds leading to $\tilde{e}^{\text{key}}_{ZX}$ are not identical to the one in the testing rounds which leads to $\tilde{e}^{\text{obs}}_{XX}$, one cannot directly use Serfling (Lemma 2) to relate the two, as we did in Section 3.3. Therefore, we introduce another set of virtual measurements (which take place in the **Key* ($X \to X$)** box in Fig. 3), corresponding to X basis second and third step measurements. Thus we obtain another error rate $\tilde{e}^{\text{key}}_{XX}$. This is the error rate corresponding to the case where these $\tilde{n}_K$ rounds are measured using $\left\{G^{\text{con,F}}_{(XX),(\neq)}, G^{\text{con,F}}_{(XX),(=)}, \mathrm{I} - F_{(X),(\text{con})}\right\}$ (the same measurement that testing rounds are subject to).

4.3 Cost of removing the basis-independent loss assumption

In removing the basis-independent loss assumption from phase error estimation, we will need to define metrics δ_1, δ_2, which will quantify the deviation from ideal behavior. We will now explain how these metrics are defined.

Consider the POVM elements $G^{\text{con,F}}_{(ZX),(\neq)}$ and $G^{\text{con,F}}_{(XX),(\neq)}$ defined via Eq. (17), which combine the second and third step measurements. In Section 3 they were exactly equal. We define δ_1 to quantify the closeness of these POVM elements as

$$\delta_1 := 2\left\|G^{\text{con,F}}_{(ZX),(\neq)} - G^{\text{con,F}}_{(XX),(\neq)}\right\|_\infty, \tag{18}$$

and use it in Lemma 3 (to be discussed later) in our proof.

Consider the second step measurements, where outcomes corresponding to POVM element $\mathrm{I} - F_{(Z),(\text{con})}$ are discarded. In Section 3, there was no need of the second step filtering measurement, which is equivalent to having $F_{(Z),(\text{con})} = \mathrm{I}$. We define δ_2 to quantify the amount of deviation from this case as

$$\delta_2 := \left\|\mathrm{I} - F_{(Z),(\text{con})}\right\|_\infty. \tag{19}$$

Thus δ_2 controls the likelihood of discards in the second step filtering measurements.

Having defined δ_1, δ_2 as metrics of the deviation from the basis-independent loss assumption, we now move on to consider the relations between the error rates in the next subsection.

4.4 Sampling

Let us recall the error-rates we have defined so far:

1. e^{obs}_X is the fraction of the n_X testing rounds that resulted in the $G^{\text{con,F}}_{(XX),(\neq)}$ outcome. We have access to e^{obs}_X in the protocol, since it is something we actually observe.

2. $\tilde{e}^{\text{obs}}_{XX}$ is the fraction of the $\tilde{n}_X$ testing rounds (after basis-independent filter only) that result in $G^{\text{con,F}}_{(XX),(\neq)}$-outcome. e^{obs}_X is obtained from $\tilde{e}^{\text{obs}}_{XX}$ after some rounds are discarded in the second step measurements.

3. $\tilde{e}^{\text{key}}_{XX}$ is the fraction of the $\tilde{n}_K$ key generation rounds (after basis-independent filter only) that result in $G^{\text{con,F}}_{(XX),(\neq)}$-outcome.

4. $\tilde{e}^{\text{key}}_{ZX}$ is the fraction of the $\tilde{n}_K$ key generation rounds (after basis-independent filter only) that result in $G^{\text{con,F}}_{(ZX),(\neq)}$-outcome.

5. e^{key}_X is the fraction of the n_K key generation rounds that result in $G^{\text{con,F}}_{(ZX),(\neq)}$-outcome. This is the quantity we wish to estimate. e^{key}_X is obtained from $\tilde{e}^{\text{key}}_{ZX}$ after some rounds are discarded in the second step measurements.

We wish to prove Eq. (5) that relate $\boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}}$ to $\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}}$. We do this by relating the various error-rates together as $\boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}} \leftrightarrow \tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{obs}} \leftrightarrow \tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{key}} \leftrightarrow \tilde{\boldsymbol{e}}_{\boldsymbol{ZX}}^{\text{key}} \leftrightarrow \boldsymbol{e}_{\boldsymbol{X}}^{\text{key}}$. We will consider the event $\Omega_{(\tilde{n}_X,\tilde{n}_K)}$, even though we do not actually observe it in the protocol. In the end, all random variables and events not directly observed in the protocol will disappear from our final expressions.

- $\boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}} \leftrightarrow \tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{obs}}$: Recall from the **Testing*($X \to X$)** node in Fig. 3, that $\boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}} = \boldsymbol{N}_{G^{\text{con,F}}_{(XX),(\neq)}}/\boldsymbol{n}_{\boldsymbol{X}}$ and $\tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{obs}} = \boldsymbol{N}_{G^{\text{con,F}}_{(XX),(\neq)}}/\tilde{\boldsymbol{n}}_{\boldsymbol{X}}$. The required relation follows from the fact that we discard rounds to go from $\tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{obs}}$ to $\boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}}$, i.e we have $\Pr(\boldsymbol{n}_{\boldsymbol{X}} \leq \tilde{\boldsymbol{n}}_{\boldsymbol{X}})_{|\Omega_{(\tilde{n}_X,\tilde{n}_K)}} = 1$. Therefore, we obtain
$$\Pr\left(\tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{obs}} \geq \boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}}\right)_{|\Omega_{(\tilde{n}_X,\tilde{n}_K)}} = 0. \tag{20}$$

- $\tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{obs}} \leftrightarrow \tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{key}}$: These error rates correspond to measurement outcomes using the *same* POVM, but with random assignment to testing vs key generation. Thus we can apply Lemma 2 (Serfling) in exactly the same manner as in Section 3.3, conditioned on the event $\Omega_{(\tilde{n}_X,\tilde{n}_K)}$. In doing so, we obtain
$$\Pr\left(\tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{key}} \geq \tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{obs}} + \gamma_{\text{serf}}\right)_{|\Omega_{(\tilde{n}_X,\tilde{n}_K)}} \leq e^{-2\gamma_{\text{serf}}^2 f_{\text{serf}}(\tilde{n}_X,\tilde{n}_K)}. \tag{21}$$
Using the definition from Eq. (13), we have
$$\gamma_{\text{serf}}^{\varepsilon_{\text{AT-a}}}(\tilde{n}_X,\tilde{n}_K) = \sqrt{\frac{\ln(1/\varepsilon_{\text{AT-a}}^2)}{2f_{\text{serf}}(\tilde{n}_X,\tilde{n}_K)}} \implies e^{-\left(\gamma_{\text{serf}}^{\varepsilon_{\text{AT-a}}}(\tilde{n}_X,\tilde{n}_K)\right)^2 2f_{\text{serf}}(\tilde{n}_X,\tilde{n}_K)} = \varepsilon_{\text{AT-a}}^2. \tag{22}$$
Therefore, we obtain
$$\Pr\left(\tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{key}} \geq \tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{obs}} + \gamma_{\text{serf}}^{\varepsilon_{\text{AT-a}}}(\tilde{n}_X,\tilde{n}_K)\right)_{|\Omega_{(\tilde{n}_X,\tilde{n}_K)}} \leq \varepsilon_{\text{AT-a}}^2 \tag{23}$$

- $\tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{key}} \leftrightarrow \tilde{\boldsymbol{e}}_{\boldsymbol{ZX}}^{\text{key}}$: We utilize the definition of δ_1 stated in Section 6.2. Since the POVM elements generating $\tilde{\boldsymbol{e}}_{\boldsymbol{ZX}}^{\text{key}}$ $(G^{\text{con,F}}_{(ZX),(\neq)})$ and $\tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{key}}$ $(G^{\text{con,F}}_{(XX),(\neq)})$ are close, we expect the bounds obtained on $\tilde{\boldsymbol{e}}_{\boldsymbol{ZX}}^{\text{key}}$ and $\tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{key}}$ to also be close. This is made precise in the following lemma proved in Section C.2.

Lemma 3. [Similar measurements lead to similar observed frequencies] Let $\rho_{Q^n} \in S_\circ(Q^{\otimes n})$ be an arbitrary state. Let $\{P, \mathrm{I}-P\}$ and $\{P', \mathrm{I}-P'\}$ be two sets of POVM elements, such that $\|P'-P\|_\infty \leq \delta$. Then,
$$\Pr\left(\frac{\boldsymbol{N}_{P'}}{n} \geq e + 2\delta + c\right) \leq \Pr\left(\frac{\boldsymbol{N}_P}{n} \geq e\right) + F(n, 2\delta, c), \tag{24}$$
for $e \in [0,1]$, where $\boldsymbol{N}_P$ is the number of P-outcomes when each subsystem of ρ_{Q^n} is measured using POVM $\{P, \mathrm{I}-P\}$, and
$$F(n,\delta,c) \coloneqq \sum_{i=n(\delta+c)}^{n} \binom{n}{i} \delta^i (1-\delta)^{n-i}. \tag{25}$$
Thus, using Lemma 3 and δ_1 defined in Eq. (18), we obtain
$$\Pr\left(\tilde{\boldsymbol{e}}_{\boldsymbol{ZX}}^{\text{key}} \geq e + \delta_1 + c_1\right)_{|\Omega_{(\tilde{n}_X,\tilde{n}_K)}} \leq \Pr\left(\tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{key}} \geq e\right)_{|\Omega_{(\tilde{n}_X,\tilde{n}_K)}} + F(\tilde{n}_K, \delta_1, c_1). \tag{26}$$
We would like $F(\tilde{n}_K,\delta_1,c_1)$ to be equal to a constant $\varepsilon_{\text{AT-b}}^2$ on the right hand side of the above expression. To do so, we note that $F(\tilde{n}_K,\delta_1,c_1)$ is a monotonic (and therefore invertible) function of c_1. Thus, we can choose c_1 to be a function $\gamma_{\text{bin}}^{\varepsilon_{\text{AT-b}}}(\tilde{n}_K,\delta_1)$ such that
$$F(\tilde{n}_K,\delta_1,\gamma_{\text{bin}}^{\varepsilon_{\text{AT-b}}}(\tilde{n}_K,\delta_1)) = \varepsilon_{\text{AT-b}}^2. \tag{27}$$

Using this as a definition $\gamma_{\text{bin}}^{\varepsilon_{\text{AT-b}}}(\tilde{n}_K, \delta_1)$, we obtain

$$\Pr\left(\tilde{\boldsymbol{e}}_{\boldsymbol{ZX}}^{\text{key}} \geq e + \delta_1 + \gamma_{\text{bin}}^{\varepsilon_{\text{AT-b}}}(\tilde{n}_K, \delta_1)\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} \leq \Pr\left(\tilde{\boldsymbol{e}}_{\boldsymbol{XX}}^{\text{key}} \geq e\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} + \varepsilon_{\text{AT-b}}^2. \tag{28}$$

Note that γ_{bin} can be easily computed numerically by relating $F(n, \delta, c)$ (and its inverse) to the cumulative binomial distribution and using root finding algorithms.

- $\tilde{\boldsymbol{e}}_{\boldsymbol{ZX}}^{\text{key}} \leftrightarrow \boldsymbol{e}_{\boldsymbol{X}}^{\text{key}}$: We will use the fact that the filtering measurements result in a very small number of discards.

  First, note that $\tilde{\boldsymbol{e}}_{\boldsymbol{ZX}}^{\text{key}} = \boldsymbol{N}_{G_{(ZX),(\neq)}^{\text{con,F}}}/\tilde{\boldsymbol{n}}_{\boldsymbol{K}}$, and $\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}} = \boldsymbol{N}_{G_{(ZX),(\neq)}^{\text{con,F}}}/\boldsymbol{n}_{\boldsymbol{K}}$. Thus, we have $\tilde{\boldsymbol{e}}_{\boldsymbol{ZX}}^{\text{key}}/\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}} = \boldsymbol{n}_{\boldsymbol{K}}/\tilde{\boldsymbol{n}}_{\boldsymbol{K}}$.

  Recall that $\boldsymbol{n}_{\boldsymbol{K}}$ is obtained by discarding rounds from $\tilde{\boldsymbol{n}}_{\boldsymbol{K}}$ based on $\{F_{(Z),(\text{con})}, \text{I} - F_{(Z),(\text{con})}\}$ measurements. We will essentially show that very few rounds are discarded in this step, using Eq. (19). To do so, we prove the following Lemma in Section C.

  Lemma 4. [Small POVM measurement] Let $\rho_{Q^n} \in S_\circ(Q^{\otimes n})$ be an arbitrary state. Let $\{P, I - P\}$ be a POVM such that $\|P\|_\infty \leq \delta$. Then

$$\Pr\left(\frac{\boldsymbol{N}_P}{n} \geq \delta + c\right) \leq F(n, \delta, c) \coloneqq \sum_{i=n(\delta+c)}^{n} \binom{n}{i} \delta^i (1-\delta)^{n-i}, \tag{29}$$

  where $\boldsymbol{N}_P$ is the number of P-outcomes when each subsystem of ρ_{Q^n} is measured using POVM $\{P, \text{I} - P\}$.

  Then, using Lemma 4 with $P = \text{I} - F_{(Z),(\text{con})}$ and δ_2 defined in Eq. (19), we obtain

$$\begin{aligned} \Pr\left(\tilde{\boldsymbol{e}}_{\boldsymbol{ZX}}^{\text{key}} \leq \boldsymbol{e}_{\boldsymbol{X}}^{\text{key}}(1 - \delta_2 - c_2)\right)_{\Omega_{(\tilde{n}_X, \tilde{n}_K)}} &= \Pr\left(\frac{\tilde{n}_K - \boldsymbol{n}_{\boldsymbol{K}}}{\tilde{n}_K} \geq \delta_2 + c_2\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} \\ &= \Pr\left(\frac{\boldsymbol{N}_{\text{I}-F_{(Z),(\text{con})}}}{\tilde{n}_K} \geq \delta_2 + c_2\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} \\ &\leq F(\tilde{n}_K, \delta_2, c_2). \end{aligned} \tag{30}$$

  Again, we would like $F(\tilde{n}_K, \delta_2, c_2)$ to be a constant value $\varepsilon_{\text{AT-c}}^2$. Thus, we replace c_2 with $\gamma_{\text{bin}}^{\varepsilon_{\text{AT-c}}}(\tilde{n}_K, \delta_2)$ and obtain

$$\Pr\left(\tilde{\boldsymbol{e}}_{\boldsymbol{ZX}}^{\text{key}} \leq \boldsymbol{e}_{\boldsymbol{X}}^{\text{key}}(1 - \delta_2 - \gamma_{\text{bin}}^{\varepsilon_{\text{AT-c}}}(\tilde{n}_K, \delta_2))\right)_{|\Omega_{(\tilde{n}_K, \tilde{n}_K)}} \leq \varepsilon_{\text{AT-c}}^2 \tag{31}$$

Thus we have relationships Eqs. (20), (23), (28) and (31) between all the error rates, whose complements hold with high probability. These can all be combined using straightforward but cumbersome algebra (see Section D), to obtain

$$\Pr\left(\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}} \geq \frac{\boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}} + \gamma_{\text{serf}}^{\varepsilon_{\text{AT-a}}}(\tilde{n}_X, \tilde{n}_K) + \delta_1 + \gamma_{\text{bin}}^{\varepsilon_{\text{AT-b}}}(\tilde{n}_K, \delta_1)}{(1 - \delta_2 - \gamma_{\text{bin}}^{\varepsilon_{\text{AT-c}}}(\tilde{n}_K, \delta_2))}\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} \leq \varepsilon_{\text{AT-b}}^2 + \varepsilon_{\text{AT-a}}^2 + \varepsilon_{\text{AT-c}}^2. \tag{32}$$

Using the above expression requires us to know the values of $\tilde{n}_K$ and $\tilde{n}_X$ which we do not. This problem is easily resolved by noting all the γs are decreasing functions of $\tilde{n}_K$ and $\tilde{n}_X$, and that $\tilde{n}_K(\tilde{n}_X)$ cannot be smaller than $n_K(n_X)$ (since we discard rounds to from the former to the latter) . Thus, we can replace $\tilde{n}_K$ with $\boldsymbol{n}_{\boldsymbol{K}}$ and $\tilde{n}_X$ with $\boldsymbol{n}_{\boldsymbol{X}}$ and obtain

$$\Pr\left(\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}} \geq \frac{\boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}} + \gamma_{\text{serf}}^{\varepsilon_{\text{AT-a}}}(\boldsymbol{n}_{\boldsymbol{X}}, \boldsymbol{n}_{\boldsymbol{K}}) + \delta_1 + \gamma_{\text{bin}}^{\varepsilon_{\text{AT-b}}}(\boldsymbol{n}_{\boldsymbol{K}}, \delta_1)}{(1 - \delta_2 - \gamma_{\text{bin}}^{\varepsilon_{\text{AT-c}}}(\boldsymbol{n}_{\boldsymbol{K}}, \delta_2))}\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} \leq \varepsilon_{\text{AT-b}}^2 + \varepsilon_{\text{AT-a}}^2 + \varepsilon_{\text{AT-c}}^2 \tag{33}$$

We set $\varepsilon_{\text{AT-a}}^2 + \varepsilon_{\text{AT-b}}^2 + \varepsilon_{\text{AT-c}}^2 = \varepsilon_{\text{AT}}^2$, and obtain the choice of $\mathcal{B}_{\delta_1,\delta_2}$:

$$\mathcal{B}_{\delta_1,\delta_2}(e_X^{\text{obs}}, n_X, n_K) \coloneqq \frac{e_X^{\text{obs}} + \gamma_{\text{serf}}^{\varepsilon_{\text{AT-a}}}(n_X, n_K) + \delta_1 + \gamma_{\text{bin}}^{\varepsilon_{\text{AT-b}}}(n_K, \delta_1)}{(1 - \delta_2 - \gamma_{\text{bin}}^{\varepsilon_{\text{AT-c}}}(n_K, \delta_2))}, \tag{34}$$

where functions $\gamma_{\text{bin}}, \gamma_{\text{serf}}$ are defined in Eq. (27) and Eq. (13) respectively. Since Eq. (33) is valid for all events $\Omega_{(\tilde{n}_X,\tilde{n}_K)}$, the above choice satisfies Eq. (5) via

$$\begin{aligned}\Pr\Big(\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}} \geq \mathcal{B}_{\delta_1,\delta_2}(\boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}}, \boldsymbol{n_X}, \boldsymbol{n_K})\Big) &\leq \sum_{\tilde{n}_X,\tilde{n}_K} \Pr\big(\Omega_{(\tilde{n}_X,\tilde{n}_K)}\big) \Pr\Big(\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}} \geq \mathcal{B}_{\delta_1,\delta_2}(\boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}}, \boldsymbol{n_X}, \boldsymbol{n_K})\Big)_{|\Omega_{(\tilde{n}_X,\tilde{n}_K)}} \\ &\leq \sum_{\tilde{n}_X,\tilde{n}_K} \Pr\big(\Omega_{(\tilde{n}_X,\tilde{n}_K)}\big)\varepsilon_{\text{AT}}^2 = \varepsilon_{\text{AT}}^2.\end{aligned} \tag{35}$$

Remark 9. Let us investigate the behavior of Eq. (34) in the limit $\delta_1, \delta_2 \to 0$. Recall that $\gamma_{\text{bin}}^{\varepsilon_{\text{AT}}}(n, \delta)$ was defined as the value of c such that $F(n, \delta, c) = \sum_{i=n(\delta+c)}^{n} \binom{n}{k}\delta^i(1-\delta)^{n-i} \leq \varepsilon_{\text{AT}}^2$. However, notice that $\delta \to 0 \implies F(n, \delta, c) \to 0$ for any value of c. Therefore, $\delta \to 0 \implies \gamma_{\text{bin}}(n, \delta) \to 0$. Setting these limits in Eq. (34), we recover the result Eq. (14) for the case where the basis-independent loss assumption is satisfied.

Thus we now have a phase error estimation bound that is valid even in the presence of basis-efficiency mismatch. We summarize the results of this section in the following theorem. Note that the results of Section 3 are a special case ($\delta_1, \delta_2 = 0$) of the following theorem.

Theorem 2 (Sampling with different filtering measurements)**.** Let $\rho_{A^nB^n} \in S_\circ(A^nB^n)$ be an arbitrary state representing n rounds of the QKD protocol. Suppose each round is assigned to test with some probability and key with some probability (and discarded with some probability).

The test rounds undergo the following measurement procedure:

1. Measurement using $\{\tilde{F}, \mathrm{I} - \tilde{F}\}$ and discarding the latter outcomes.
2. Measurement using $\{F_{\text{con}}^{\text{test}}, \mathrm{I} - F_{\text{con}}^{\text{test}}\}$ and discarding the latter outcomes. We let $\boldsymbol{n_T}$ be the number of remaining rounds at this stage.
3. Measurement using $\{G_{\neq}^{\text{test}}, G_{=}^{\text{test}}\}$. We let $\boldsymbol{e}^{\text{obs}} = \boldsymbol{N}_{G_{\neq}^{\text{test}}}/\boldsymbol{n_T}$ be the error rate in these rounds.

The key generation rounds undergo the following measurement procedure:

1. Measurement using $\{\tilde{F}, \mathrm{I} - \tilde{F}\}$ and discarding the latter outcomes.
2. Measurement using $\{F_{\text{con}}^{\text{key}}, \mathrm{I} - F_{\text{con}}^{\text{key}}\}$ and discarding the latter outcomes. We let $\boldsymbol{n_K}$ be the number of remaining rounds at this stage.
3. Measurement using $\{G_{\neq}^{\text{key}}, G_{=}^{\text{key}}\}$. We let $\boldsymbol{e}^{\text{key}} = \boldsymbol{N}_{G_{\neq}^{\text{key}}}/\boldsymbol{n_K}$ be the error rate in these rounds.

Then, the following equation holds

$$\Pr\big(\boldsymbol{e}^{\text{key}} \geq \mathcal{B}_{\delta_1,\delta_2}(\boldsymbol{e}^{\text{obs}}, \boldsymbol{n_T}, \boldsymbol{n_K})\big) \leq \varepsilon_{\text{AT-a}}^2 + \varepsilon_{\text{AT-b}}^2 + \varepsilon_{\text{AT-c}}^2, \tag{36}$$

where

$$\begin{aligned}\mathcal{B}_{\delta_1,\delta_2}(e^{\text{obs}}, n_T, n_K) &= \frac{e^{\text{obs}} + \gamma_{\text{serf}}^{\varepsilon_{\text{AT-a}}}(n_T, n_K) + \delta_1 + \gamma_{\text{bin}}^{\varepsilon_{\text{AT-b}}}(n_K, \delta_1)}{(1 - \delta_2 - \gamma_{\text{bin}}^{\varepsilon_{\text{AT-c}}}(n_K, \delta_2))}, \\ \delta_1 &= 2\left\|\sqrt{F_{\text{con}}^{\text{key}}}G_{\neq}^{\text{key}}\sqrt{F_{\text{con}}^{\text{key}}} - \sqrt{F_{\text{con}}^{\text{test}}}G_{\neq}^{\text{test}}\sqrt{F_{\text{con}}^{\text{test}}}\right\|_\infty, \\ \delta_2 &= \left\|\mathrm{I} - F_{\text{con}}^{\text{key}}\right\|_\infty,\end{aligned} \tag{37}$$

and $\gamma_{\text{bin}}, \gamma_{\text{serf}}$ are defined in Eq. (27) and Eq. (13) respectively.

Proof sketch. The rigorous proof follows from the analysis already seen in Section 4. Essentially, we consider several error rates corresponding to various measurement choices, as described in Fig. 3, and use Lemmas 2 to 4 to relate the various error rates together.

Remark 10. Note that in our analysis in this section, we actually had $G_{\neq}^{\text{key}} = G_{\neq}^{\text{test}}$, i.e the third step measurements were identical in the key and test rounds. However, our result holds even if these measurements are different, by going through the same steps in the proof. Hence, we state Theorem 2 in full generality.

5 Application to Decoy-state BB84

So far in this work, we have focused our attention on the BB84 protocol implemented using perfect single-photon sources for pedagogical reasons. In this section, we will extend our techniques and obtain a variable-length security proof for decoy-state BB84 [42–46] with imperfect detectors. We base our security proof approach on that of Lim et al [35], with the following differences.

First, we rigorously prove the security for the variable-length decoy-state BB84 protocol in the entropic uncertainty relations framework (note that Ref. [35] actually implicitly implements a variable-length protocol). In fact [35] considers a protocol with iterative sifting [6] where the total number of rounds in the protocol is not fixed a priori, and depends on observations made during the protocol, which are announced in a round-by-round manner. However a justification for this step is not provided. This is important because certain kinds of iterative sifting can lead to subtle issues in the security analysis (see Ref. [47] for some issues and Ref. [48] for solutions). We do not fix this problem directly in this work. Instead, we consider a protocol with a fixed total number of signals sent, which avoids this problem. Second, we make rigorous certain technical steps in [35] (regarding entropic calculations on states conditioned on events), which we point out where applicable (see Remark 21). Third, our phase error estimates do not require the assumption of basis-independent loss unlike that of [35]. We also avoid a particular Taylor series approximation used by [35] ([49, Eq. 22]), and therefore our phase error estimation procedure yields a true bound without any approximations. Finally we also clarify certain aspects of the decoy analysis undertaken in [35]. In particular, we careful differentiate between random variables and an observed value of the random variable, and also properly condition on relevant events in our presentation. We stress that while we clarify and make rigorous certain steps in [35] (see also [4, Section 6.1]), our main contribution in this work is the variable-length security proof of decoy-state BB84 in the presence of detector imperfections.

Remark 11. Recently, a more accessible version of the security proof in Ref. [35] was written in Ref. [50]. While Ref. [50][Version 2] addresses many of the above concerns for fixed-length protocols, it does not deal with detector imperfections or variable-length protocols.

We start by first specifying the decoy-state BB84 protocol we study in Section 5.1. We will then explain the required bounds on the phase error rate in Section 5.2. We explain decoy analysis in Section 5.3, and state the security of our variable-length protocol in Section 5.5. Some proofs are delegated to Section E.

5.1 Protocol specification

The decoy-state BB84 protocol modifies the following steps of the protocol described in Section 2.

1. **State Preparation:** Alice decides to send states in the $Z(X)$ basis with probability $p^{(A)}_{(Z)}$ ($p^{(A)}_{(X)}$). She additionally chooses a signal intensity $\mu_k \in \{\mu_1, \mu_2, \mu_3\}$ with some predetermined probability p_{μ_k} [7]. She prepares a phase-randomized weak laser pulse based on the chosen values, and sends the state to Bob. We assume $\mu_1 > \mu_2 + \mu_3$ and $\mu_2 > \mu_3 \geq 0$. This requirement on the intensity values, as well as the total number of intensities, is not fundamental. It is used in deriving the analytical bounds in the decoy-state analysis.

2. **Measurement:** Bob chooses basis the basis $Z(X)$ with probability with $p^{(B)}_{(Z)}(p^{(B)}_{(X)})$ and measures the incoming state. This step of the protocol is identical to Section 2.

3. **Classical Announcements and Sifting:** For all rounds, Alice and Bob announce the basis they used. Furthermore, Bob announces whether he got a conclusive outcome ($\{\Gamma^{(B)}_{(b,0)}, \Gamma^{(B)}_{(b,1)}\}$), or an inconclusive outcome ($\{\Gamma^{(B)}_{(b,\perp)}\}$). A round is said to be "conclusive" if Alice and Bob used the same basis, and Bob obtained a conclusive outcome.

[6] This has been formulated in a variety of ways in the literature. In general, we use this phrase for protocols that have a loop phase, where some actions are taken repeatedly until certain conditions are met.

[7] This probability can depend on the basis used without affecting the results of this work. To incorporate this, one simply has to track the correct probability distribution through all the calculations.

On all the X basis conclusive rounds, Alice and Bob announce their measurement outcomes and intensity choices. We let n_{X,μ_k} be the number of X basis conclusive rounds where Alice chose intensity μ_k, and let e^{obs}_{X,μ_k} be the observed error rate in these rounds. For brevity, we use the notation $n_{X,\mu_{\vec{k}}} = (n_{X,\mu_1} \dots n_{X,\mu_3})$ to denote observations from all intensities. (We use similar notation for $e^{\text{obs}}_{X,\mu_{\vec{k}}}$, $n_{K,\mu_{\vec{k}}}$ etc).

On all Z basis conclusive round, Alice and Bob announce their measurement outcomes with some small probability $p_{\text{Z,T}}$. We let e^{obs}_Z denote the observed error rate in these rounds (intensity is ignored), which is used to determine the amount of error-correction that needs to be performed. For the remaining n_K rounds, Alice announces her intensity choices, and these rounds are used for key generation.

All announcements are stored in the register C^n. We use $\Omega_{(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_Z)}$ to denote the event that $n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_Z$ values are observed in the protocol.

The remaining steps of the protocol are the same as in Section 2. In particular, based on the observations $n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_Z$, Alice and Bob implement one-way error-correction using $\lambda_{\text{EC}}(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_Z)$ bits of communication, followed by error-verification, and privacy amplification to produce a key of $l(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_Z)$ bits. This requirement of one-way communication is not fundamental, and more complicated error-correction protocols can be accommodated in a straightforward manner (see Remark 4). Additionally note that our protocol generates key from *all* intensities, instead of having a single "signal" intensity for key generation.

5.2 Required and actual phase error estimation bound

In order to prove security for our decoy-state QKD protocol, we will need to bound two quantities. First, we must obtain a lower bound on the number of single-photon events that lead to key generation $\boldsymbol{n_{K,1}}$. Second, we must obtain an upper bound on the phase error rate within these single-photon key generation rounds, given by $\boldsymbol{e^{\text{key}}_{X,1}}$. This can be represented mathematically as

$$\Pr\Big(\boldsymbol{e^{\text{key}}_{X,1}} \geq \mathcal{B}_e(\boldsymbol{e^{\text{obs}}_{X,\mu_{\vec{k}}}}, \boldsymbol{n_{X,\mu_{\vec{k}}}}, \boldsymbol{n_{K,\mu_{\vec{k}}}}) \quad \vee \quad \boldsymbol{n_{K,1}} \leq \mathcal{B}_1(\boldsymbol{n_{K,\mu_{\vec{k}}}})\Big) \leq \varepsilon^2_{\text{AT}}, \tag{38}$$

where $\vee$ denotes the logical OR operator, and $\mathcal{B}_e, \mathcal{B}_1$ are functions that provide these bounds as a function of the observed values.

This statement will be used in the proof of Theorem 3 to prove the variable-length security of our protocol. We will derive the required bounds $(\mathcal{B}_e, \mathcal{B}_1)$ in Eq. (38) in two steps. First we will use decoy analysis to convert from observations corresponding to different intensities (which we have access to) to those corresponding to different photon numbers (which we do not have access to). We will be concerned with three outcomes $\{X_{\neq}, X, K\}$, corresponding to X basis conclusive error outcome, X basis conclusive outcome, and Z basis conclusive outcome used for key generation respectively. Thus, at the end of the first step we will obtain

$$\Pr\left(\boldsymbol{e^{\text{obs}}_{X,1}} \geq \frac{\mathcal{B}^{\text{decoy}}_{\text{max}-1}(\boldsymbol{n_{X_{\neq},\mu_{\vec{k}}}})}{\mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n_{X,\mu_{\vec{k}}}})} \quad \vee \quad \boldsymbol{n_{X,1}} \leq \mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n_{X,\mu_{\vec{k}}}}) \quad \vee \quad \boldsymbol{n_{K,1}} \leq \mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n_{K,\mu_{\vec{k}}}})\right) \leq 9\varepsilon^2_{\text{AT-d}} \tag{39}$$

where $\mathcal{B}^{\text{decoy}}_{\text{min}-m}$ and $\mathcal{B}^{\text{decoy}}_{\text{max}-m}$ are functions that compute bounds on the m-photon components of the input statistics. Note that we use $\boldsymbol{n_{X_{\neq},\mu_{\vec{k}}}} = (\boldsymbol{n_{X,\mu_1}} \times \boldsymbol{e^{\text{obs}}_{X,\mu_1}}, \dots, \boldsymbol{n_{X,\mu_3}} \times \boldsymbol{e^{\text{obs}}_{X,\mu_3}})$ to denote the number of rounds resulting both Alice and Bob using the X basis and obtaining an error, for each intensity (and we will assume implicit conversion between these two notations). The 9 on the RHS comes from the fact that we implement decoy analysis on 3 different events and we have 3 intensities. We will prove Eq. (39) in Section 5.3.

Remark 12. Note that the only parameters actually observed in the protocol are given by $n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_Z$. Variables like $\boldsymbol{e^{\text{obs}}_{X,1}}$ are not actually directly observed, but instead are derived from observations.

In this second step, we will use $\boldsymbol{e}^{\text{obs}}_{\boldsymbol{X},\boldsymbol{1}}, \boldsymbol{n}_{\boldsymbol{X},\boldsymbol{1}}, \boldsymbol{n}_{\boldsymbol{K},\boldsymbol{1}}$ to bound the single photon phase error rate $\boldsymbol{e}^{\text{key}}_{\boldsymbol{X},\boldsymbol{1}}$. Notice this is exactly what we showed Sections 3 and 4. In particular, with $\mathcal{B}_{\delta_1,\delta_2}$ directly obtained from Eq. (34), we have

$$\Pr\left(\boldsymbol{e}^{\text{key}}_{\boldsymbol{X},\boldsymbol{1}} \geq \mathcal{B}_{\delta_1,\delta_2}(\boldsymbol{e}^{\text{obs}}_{\boldsymbol{X},\boldsymbol{1}}, \boldsymbol{n}_{\boldsymbol{X},\boldsymbol{1}}, \boldsymbol{n}_{\boldsymbol{K},\boldsymbol{1}})\right) \leq \varepsilon^2_{\text{AT-s}}. \tag{40}$$

where $\varepsilon^2_{\text{AT-s}}$ denotes the failure probability of the "single-photon" part of our estimation.

However, note that we do not directly observe $\boldsymbol{e}^{\text{obs}}_{\boldsymbol{X},\boldsymbol{1}}, \boldsymbol{n}_{\boldsymbol{X},\boldsymbol{1}}, \boldsymbol{n}_{\boldsymbol{K},\boldsymbol{1}}$ in the decoy-state protocol (unlike Section 4). Thus we would like to replace these values with the bounds computed from our decoy analysis (Eq. (39)). This is straightforward to do, since $\mathcal{B}_{\delta_1,\delta_2}$ is an increasing function of $\boldsymbol{e}^{\text{obs}}_{\boldsymbol{X},\boldsymbol{1}}$, and decreasing function of $\boldsymbol{n}_{\boldsymbol{X},\boldsymbol{1}}, \boldsymbol{n}_{\boldsymbol{K},\boldsymbol{1}}$. This can be done formally by a straightforward application of the union bound for probabilities ($\Pr(\Omega_1 \vee \Omega_2) \leq \Pr(\Omega_1) + \Pr(\Omega_2)$) applied to Eqs. (39) and (40). Doing so allows us to conclude that the probability of *any* of the bounds in Eqs. (39) and (40) failing is smaller than $9\varepsilon^2_{\text{AT-d}} + \varepsilon^2_{\text{AT-s}}$. Then we use the fact that if *none* of the bounds inside the probabilities in Eqs. (39) and (40) fail, then this implies that the bounds inside the probability in Eq. (41) below must hold. Formally, we obtain

$$\begin{aligned}\Pr\Bigg(\boldsymbol{e}^{\text{key}}_{\boldsymbol{X},\boldsymbol{1}} \geq \mathcal{B}_{\delta_1,\delta_2}\left(\frac{\mathcal{B}^{\text{decoy}}_{\text{max}-1}(\boldsymbol{n}_{\boldsymbol{X}\neq,\boldsymbol{\mu}_{\vec{\boldsymbol{k}}}})}{\mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n}_{\boldsymbol{X},\boldsymbol{\mu}_{\vec{\boldsymbol{k}}}})}, \mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n}_{\boldsymbol{X},\boldsymbol{\mu}_{\vec{\boldsymbol{k}}}}), \mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n}_{\boldsymbol{K},\boldsymbol{\mu}_{\vec{\boldsymbol{k}}}})\right) \quad \vee \\ \boldsymbol{n}_{\boldsymbol{K},\boldsymbol{1}} \leq \mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n}_{\boldsymbol{K},\boldsymbol{\mu}_{\vec{\boldsymbol{k}}}})\Bigg) \leq 9\varepsilon^2_{\text{AT-d}} + \varepsilon^2_{\text{AT-s}} =: \varepsilon^2_{\text{AT}}\end{aligned} \tag{41}$$

which is the required statement. Thus, it is now enough to prove Eq. (39) in order to prove Eq. (41) (equivalently Eq. (38)), for which we turn to decoy analysis in the next section.

5.3 Decoy Analysis

Let O denote a specific outcome of a given round, and let n_O denote the number of rounds that resulted in the outcome O. For instance, it could denote that both Alice and Bob measured in the X basis and obtained a detection (in which case $n_O = n_X$). We will perform a general decoy analysis for any outcome O. Let n_{O,μ_k} denote the number of rounds that resulted in the outcome O where Alice used intensity μ_k. We have access to this information during the protocol. Let $n_{O,m}$ denote the number of rounds that resulted in the outcome O where Alice prepared a state of m photons. We wish to obtain bounds on $n_{O,m}$ using n_{O,μ_k}.

In practice, Alice first chooses an intensity μ_k of the pulse, which then determines the photon number m of the pulse, via the Poissonian distribution, independently for each round. Thus we have

$$p_{m|\mu_k} = e^{-\mu_k}\frac{\mu_k^m}{m!}. \tag{42}$$

The probability of m-photons being emitted, can be obtained via

$$\tau_m = \sum_{\mu_k} p_{\mu_k} p_{m|\mu_k} = \sum_{\mu_k} p_{\mu_k} e^{-\mu_k}\frac{\mu_k^m}{m!}. \tag{43}$$

Now, without loss of generality, we can view Alice as *first* choosing the photon number m, and *then* choosing a intensity setting μ_k with probability given by

$$p_{\mu_k|m} = p_{\mu_k} p_{m|\mu_k}/\tau_m. \tag{44}$$

This is the fundamental idea used by [35, 45, 46]. In this case, due to the fact that each signal is mapped to an intensity independently of other signals, one can apply the Hoeffdings inequality to these independent events, and obtain

$$\Pr\left(\left|\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_k}} - \sum_{m=0}^{\infty} p_{\mu_k|m}\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{m}}\right| \geq \sqrt{\frac{\boldsymbol{n}_{\boldsymbol{O}}}{2}\ln\left(\frac{2}{\varepsilon^2_{\text{AT-d}}}\right)}\right) \leq \varepsilon^2_{\text{AT-d}}. \tag{45}$$

Remark 13. The application of Hoeffdings inequality here is subtle, and is made rigorous in Lemmas 13 and 14 in Section E (see also Ref. [46]). Note that in general, the photon numbers of every pulse in the protocol are chosen independently, since Alice chooses intensity independently for each pulse. However, here we are interested in photon numbers corresponding to rounds that led to a specific outcome O. Since we postselect pulses based on the outcome, we can no longer claim that the photon numbers of these pulses (pulses that led to outcome O) are sampled independently, or that intensities of these pulses are chosen independently. This is because they now depend on Eve's attack. Rather, Lemmas 13 and 14 rely on exploiting the fact that conditioned on *any fixed sequence* of photon numbers of the pulses, the intensities are chosen independently of one another. One can therefore apply Hoeffdings inequality. Then, since the resulting statements holds for any fixed sequence of photon numbers, the conditioning on this event can be removed.

We can now combine Eq. (45) for all intensities μ_k using the union bounds for probabilities ($\Pr(\Omega_1 \wedge \Omega_2) \geq 1 - \Pr(\Omega_1^c) - \Pr(\Omega_2^c)$). Reformulating the expressions, we obtain

$$\Pr\left(\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_k}} - \sqrt{\frac{\boldsymbol{n}_{\boldsymbol{O}}}{2}\ln\left(\frac{2}{\varepsilon_{\text{AT-d}}^2}\right)} \leq \sum_{m=0}^{\infty} p_{\mu_k|m}\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{m}} \leq \boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_k}} + \sqrt{\frac{\boldsymbol{n}_{\boldsymbol{O}}}{2}\ln\left(\frac{2}{\varepsilon_{\text{AT-d}}^2}\right)} \quad \forall k \in \{1,2,3\}\right) \geq 1 - 3\varepsilon_{\text{AT-d}}^2. \tag{46}$$

To obtain Eq. (39), we will apply decoy analysis (Eq. (46)) for three separate events: conclusive Z basis rounds selected for key generation (denoted by K), conclusive X basis rounds (denoted by X), and conclusive X basis rounds leading to an error (denoted by $X_{\neq}$). Then, Eq. (46) can be applied these events (again using the union bound for probabilities) to obtain:

$$\Pr\left(\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_k}} - \sqrt{\frac{\boldsymbol{n}_{\boldsymbol{O}}}{2}\ln\left(\frac{2}{\varepsilon_{\text{AT-d}}^2}\right)} \leq \sum_{m=0}^{\infty} p_{\mu_k|m}\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{m}} \leq \boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_k}} + \sqrt{\frac{\boldsymbol{n}_{\boldsymbol{O}}}{2}\ln\left(\frac{2}{\varepsilon_{\text{AT-d}}^2}\right)} \quad \forall k \in \{1,2,3\}, \quad \forall O \in \{X_{\neq}, X, K\}\right) \geq 1 - 9\varepsilon_{\text{AT-d}}^2. \tag{47}$$

Let $\mathcal{S}_{\text{constraints}}$ denote the set of inequalities inside the probability in the above expressions. Therefore we have $\Pr(\mathcal{S}_{\text{constraints}}) \geq 1 - 9\varepsilon_{\text{AT-d}}^2$.

5.4 Bounds on zero and one photon statistics

For any event $O \in \{X, X_{\neq}, K\}$, the relevant bounds on the zero-photon and single-photon components can be obtained by algebraic manipulation of the expressions in $\mathcal{S}_{\text{constraints}}$. In general, any method for bounding the relevant zero-photon and single-photon components using $\mathcal{S}_{\text{constraints}}$ suffices. In this work, we follow exactly the steps taken by Ref. [35, Appendix A] to obtain these bounds. Thus, we only write the final expressions here. We define

$$\boldsymbol{n}^{\pm}_{\boldsymbol{O},\boldsymbol{\mu_k}} := \frac{e^{\mu_k}}{p_{\mu_k}}\left(\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_k}} \pm \sqrt{\frac{\boldsymbol{n}_{\boldsymbol{O}}}{2}\ln\left(\frac{2}{\varepsilon_{\text{AT-d}}^2}\right)}\right) \tag{48}$$

The lower bound on the zero-photon component is given by [35, Eq. 2]

$$\mathcal{S}_{\text{constraints}} \implies \boldsymbol{n}_{\boldsymbol{O},\boldsymbol{0}} \geq \mathcal{B}^{\text{decoy}}_{\text{min}-0}(\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_{\vec{k}}}}) := \tau_0 \frac{\mu_2 \boldsymbol{n}^{-}_{\boldsymbol{O},\boldsymbol{\mu_3}} - \mu_3 \boldsymbol{n}^{+}_{\boldsymbol{O},\boldsymbol{\mu_2}}}{\mu_2 - \mu_3}. \tag{49}$$

The lower bound on the one-photon component is given by [35, Eq. 3]

$$\mathcal{S}_{\text{constraints}} \implies \boldsymbol{n}_{\boldsymbol{O},\boldsymbol{1}} \geq \mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_{\vec{k}}}}) := \left(\frac{\mu_1\tau_1}{\mu_1(\mu_2-\mu_3) - \mu_2^2 + \mu_3^2}\right) \times \left(\boldsymbol{n}^{-}_{\boldsymbol{O},\boldsymbol{\mu_2}} - \boldsymbol{n}^{+}_{\boldsymbol{O},\boldsymbol{\mu_3}} - \frac{\mu_2^2 - \mu_3^2}{\mu_1^2}\left(\boldsymbol{n}^{+}_{\boldsymbol{O},\boldsymbol{\mu_1}} - \mathcal{B}^{\text{decoy}}_{\text{min}-0}(\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_{\vec{k}}}})/\tau_0\right)\right). \tag{50}$$

The upper bound on the one-photon component is given by [35, Eq. 4]

$$\mathcal{S}_{\text{constraints}} \implies \boldsymbol{n_{O,1}} \leq \mathcal{B}^{\text{decoy}}_{\text{max}-1}(\boldsymbol{n_{O,\mu_{\vec{k}}}}) \coloneqq \tau_1 \frac{\boldsymbol{n^{+}_{O,\mu_2}} - \boldsymbol{n^{-}_{O,\mu_3}}}{\mu_2 - \mu_3}. \tag{51}$$

Since $\Pr(\mathcal{S}_{\text{constraints}}) \geq 1 - 9\varepsilon^2_{\text{AT-d}}$, and Eqs. (49) to (51) follow from the expressions in $\mathcal{S}_{\text{constraints}}$, we obtain

$$\Pr\left(\boldsymbol{e^{\text{obs}}_{X,1}} \geq \frac{\mathcal{B}^{\text{decoy}}_{\text{max}-1}(\boldsymbol{n_{X\neq,\mu_{\vec{k}}}})}{\mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n_{X,\mu_{\vec{k}}}})} \quad \vee \quad \boldsymbol{n_{X,1}} \leq \mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n_{X,\mu_{\vec{k}}}}) \quad \vee \quad \boldsymbol{n_{K,1}} \leq \mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n_{K,\mu_{\vec{k}}}})\right) \leq 9\varepsilon^2_{\text{AT-d}} \tag{52}$$

5.5 Variable-length security statement for decoy-state

Having proved Eq. (38), we now have the following theorem regarding variable-length security of the decoy-state BB84 protocol.

Theorem 3. [Variable-length security of decoy-state BB84] Suppose Eq. (38) is satisfied and let $\lambda_{\text{EC}}(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_{Z})$ be a function that determines the number of bits used for error-correction in the QKD protocol. Define

$$\begin{aligned} l(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_{Z}) \coloneqq \max\Bigg(0, \mathcal{B}_1\left(n_{K,\mu_{\vec{k}}}\right)\left(1 - h\left(\mathcal{B}_e\left(e^{\text{obs}}_{X,\mu_{\vec{k}}}, n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}\right)\right)\right) \\ - \lambda_{\text{EC}}(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_{Z}) - 2\log(1/2\varepsilon_{\text{PA}}) - \log(2/\varepsilon_{\text{EV}})\Bigg) \end{aligned} \tag{53}$$

where $h(x)$ is the binary entropy function for $x \leq 1/2$, and $h(x) = 1$ otherwise. Then the variable-length decoy-state QKD protocol that produces a key of length $l(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_{Z})$ using $\lambda_{\text{EC}}(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_{Z})$ bits for error-correction, upon the event $\Omega_{(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_{Z})} \wedge \Omega_{\text{EV}}$ is $(2\varepsilon_{\text{AT}} + \varepsilon_{\text{PA}} + \varepsilon_{\text{EV}})$-secure.

Remark 14. The decoy bounds used in this work requires the use of three total intensities to provide usable bounds. Later, this was improved to only require two total intensities in Ref. [51] (see also [52] for recent improvements in decoy analysis). In this work we did *not* follow the two intensities analysis of [51]. This is due to complications stemming from the fact that this improved analysis requires the knowledge of error rates in the key generation rounds for various intensities (which is not announced). Although this issue can be resolved with additional reasoning, addressing it would divert from the primary focus of this work (which is imperfect detectors).

For instance, one way to avoid this problem is to argue that Bob can compare his raw key before and after error-correction to calculate the number of errors in the key generation rounds (assuming error-correction succeeded). This can indeed be made rigorous by arguing that if error-correction fails, the protocol aborts with high probability anyway (due to error-verification). However an additional issue remains. For variable-length protocols, Bob must *announce* either the number of errors he observes, or the length of key he wishes to produce, to Alice. This additional announcement leaks information to Eve which must be accounted for. Assuming that Bob announces the final output key length, a naive analysis would reduce the key length by an additional $\log(n_{\text{len}})$ where n_{len} denotes the number of allowed output key length. These observations are missing in Ref. [51].

Note that this problem is avoided by this work since the length of output key is a function only of the public announcements during Step 3 of the protocol (Section 5.1).

6 Results

We will now apply our results to a decoy-state BB84 protocol with realistic detectors. To do so, we start by outlining a recipe for using this work to compute key rates in Section 6.1. We will

then specify the canonical model for our detectors with efficiency mismatch in Section 6.3. We will apply the recipe to our model in Section 6.4. Finally, we will plot the key rate we obtain in Section 6.5.

6.1 Recipe for computing key rates in the presence of basis-efficiency mismatch

In this subsection, we provide straightforward instructions for using the results of this work to compute key rates for decoy-state BB84 in the presence of basis-efficiency mismatch (see the end of this subsection for a pointer to the exact expressions). We will start by explaining the computation of (upper bounds on) δ_1, δ_2 for a given model of the measurement POVMs in the protocol. To do so, one has to break up the measurement process implemented by Alice and Bob into multiple steps via multiple uses of Lemma 1. This is done as follows:

1. Start with POVM $\{\Gamma_{(b_A,b_B),(\neq)}, \Gamma_{(b_A,b_B),(=)}, \Gamma_{(b_A,b_B),(\perp)}\}$ which describe Alice and Bob measuring in the (b_A, b_B) basis, and obtaining a conclusive error, a conclusive no-error, and an inconclusive outcome respectively. (In this work, we apply this recipe on the POVMs defined in Eq. (58).)

2. Pick a $\tilde{F} \geq \Gamma_{(b_A,b_B),(\neq)} + \Gamma_{(b_A,b_B),(=)}$ for all (b_A, b_B). Consider the four-outcome POVM $\{\mathrm{I}-\tilde{F}, \tilde{F}-\Gamma_{(b_A,b_B),(=)}-\Gamma_{(b_A,b_B),(\neq)}, \Gamma_{(b_A,b_B),(=)}, \Gamma_{(b_A,b_B),(\neq)}\}$. Group the last three outcomes together, and use Lemma 1 to divide this measurement into two steps. In the first step, $\{\tilde{F}, \mathrm{I}-\tilde{F}\}$ is measured and latter outcomes discarded. The remaining rounds are measured using $\{\tilde{F}_{(b_A,b_B),(\perp)}, \tilde{F}_{(b_A,b_B),(=)}, \tilde{F}_{(b_A,b_B),(\neq)}\}$ where

$$\begin{aligned}
\tilde{F}_{(b_A,b_B),(\perp)} &= \sqrt{\tilde{F}}^{+}(\tilde{F} - \Gamma_{(b_A,b_B),(\neq)} - \Gamma_{(b_A,b_B),(\neq)})\sqrt{\tilde{F}}^{+} + \mathrm{I} - \Pi_{\tilde{F}} \\
\tilde{F}_{(b_A,b_B),(\neq)} &= \sqrt{\tilde{F}}^{+}\Gamma_{(b_A,b_B),(\neq)}\sqrt{\tilde{F}}^{+} \\
\tilde{F}_{(b_A,b_B),(=)} &= \sqrt{\tilde{F}}^{+}\Gamma_{(b_A,b_B),(=)}\sqrt{\tilde{F}}^{+}
\end{aligned} \tag{54}$$

   where $\Pi_{\tilde{F}}$ denotes the projector onto the support of $\tilde{F}$.

3. Consider the new POVM $\{\tilde{F}_{(b_A,b_B),(\perp)}, \tilde{F}_{(b_A,b_B),(=)}, \tilde{F}_{(b_A,b_B),(\neq)}\}$. Using Lemma 1 again, divide this POVM measurement into two steps. The first step is implemented using $\{F_{(b_A,b_B),(\mathrm{con})}, F_{(b_A,b_B),(\perp)}\}$ and decides whether the outcome is conclusive or inconclusive. The conclusive outcomes are further measured using $\{G^{\mathrm{con}}_{(b),(\neq)}, G^{\mathrm{con}}_{(b),(=)}\}$. These POVM elements are given by

$$\begin{aligned}
F_{(b_A,b_B),(\mathrm{con})} &= \tilde{F}_{(b_A,b_B),(\neq)} + \tilde{F}_{(b_A,b_B),(=)} \\
F_{(b_A,b_B),(\perp)} &= \tilde{F}_{(b_A,b_B),(\perp)} \\
G^{\mathrm{con}}_{(b_A,b_B),(\neq)} &= \sqrt{F_{(b_A,b_B),(\mathrm{con})}}^{+}\tilde{F}_{(b_A,b_B),(\neq)}\sqrt{F_{(b_A,b_B),(\mathrm{con})}}^{+} \\
G^{\mathrm{con}}_{(b_A,b_B),(=)} &= \sqrt{F_{(b_A,b_B),(\mathrm{con})}}^{+}\tilde{F}_{(b_A,b_B),(=)}\sqrt{F_{(b_A,b_B),(\mathrm{con})}}^{+} + \mathrm{I} - \Pi_{F_{(b_A,b_B),(\mathrm{con})}} \quad (= \mathrm{I} - G^{\mathrm{con}}_{(b_A,b_B),(\neq)})
\end{aligned} \tag{55}$$

   where $\Pi_{F_{(b_A,b_B),(\mathrm{con})}}$ is the projector onto the support of $F_{(b_A,b_B),(\mathrm{con})}$. This projector plays a trivial rule in the measurement itself, and is only included to ensure that we obtain a valid POVM.

4. Compute

$$\begin{aligned}
\delta_1 &= 2\left\| \sqrt{F_{(Z),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(X),(\mathrm{con})}} \right\|_{\infty} \\
\delta_2 &= \left\| \mathrm{I} - F_{(Z),(\mathrm{con})} \right\|_{\infty}
\end{aligned} \tag{56}$$

   where we recall that whenever the basis is explicitly written as X/Z, it represents both Alice and Bobs basis choices.

5. For the analysis of practical scenarios, where η_{b_i}, d_{b_i} are not known exactly but are instead known to be in some range, one must also additionally maximize Eq. (56) over all possible choices of η_{b_i}, d_{b_i}.

Once δ_1, δ_2 are computed via the procedure above, we can compute key rates as follows. The key rate expression for the decoy-state BB84 protocol is given by Eq. (53). To use this expression, refer to Eqs. (38) and (41) (which are notationally equivalent). The bounds for the decoy analysis in Eq. (41) are in turn found in Eqs. (49) to (51), whereas the bound for the phase error estimation is found in Eq. (34). For the BB84 protocol where Alice sends single photons, the key rate is given by Eqs. (6) and (34).

6.2 Assumptions

Note that the recipe is derived for the BB84 protocol (qubit or decoy-state) under the assumption that Alice's source is perfect. That is, Alice sends either perfect qubit BB84 states, or perfectly phase-randomized weak coherent pulses for the decoy-state protocol. The recipe is valid for all active-choice detector models, and yields non-trivial results as long as one can suitably bound δ_1, δ_2. For the explicit calculations in this work, we consider the canonical model of detectors in the next section, and then compute the values of δ_1, δ_2 for this model in Section 6.4. Therefore, the bounds in Eq. (60) are derived assuming that Bob's detector POVMs are given by Eq. (57) and characterized upto Eq. (59).

6.3 Detector Model

In this section, we specify the canonical model of Bob's detectors (for active BB84) we use in this work. Let η_{b_i}, d_{b_i} denote the efficiency and dark count rate of Bob's POVM corresponding to basis b, and bit i. We first define Bob's double click POVM for basis $b \in \{Z, X\}$ to be $\Gamma^{(B)}_{(b,\mathrm{dc})} = \sum_{N_0,N_1=0}^{\infty}(1-(1-d_{b_0})(1-\eta_{b_0})^{N_0})(1-(1-d_{b_1})(1-\eta_{b_1})^{N_1})\,|N_0,N_1\rangle\langle N_0,N_1|_b$, where $|N_0,N_1\rangle\langle N_0,N_1|_b$ is the state with N_0 photons in the mode 1, and N_1 photons in mode 2, where the modes are defined with respect to basis b. For example, for polarization-encoded BB84, $|2,1\rangle\langle 2,1|_Z$ would signify the state with 2 horizontally-polarised photons and 1 vertically polarised photon. Recall that double clicks are mapped to single clicks randomly in our protocol. Thus, we can write Bob's POVM elements as

$$\begin{aligned}
\Gamma^{(B)}_{(b,\perp)} &= \sum_{N_0,N_1=0}^{\infty}(1-d_{b_0})(1-d_{b_1})(1-\eta_{b_0})^{N_0}(1-\eta_{b_1})^{N_1}\,|N_0,N_1\rangle\langle N_0,N_1|_b \\
\Gamma^{(B)}_{(b,0)} &= (1-d_{b_1})\sum_{N_0,N_1=0}^{\infty}(1-(1-d_{b_0})(1-\eta_{b_0})^{N_0})(1-\eta_{b_1})^{N_1}\,|N_0,N_1\rangle\langle N_0,N_1|_b + \frac{1}{2}\Gamma^{(B)}_{(b,\mathrm{dc})} \qquad (57)\\
\Gamma^{(B)}_{(b,1)} &= (1-d_{b_0})\sum_{N_0,N_1=0}^{\infty}(1-\eta_{b_0})^{N_0}(1-(1-d_{b_1})(1-\eta_{b_1})^{N_1})\,|N_0,N_1\rangle\langle N_0,N_1|_b + \frac{1}{2}\Gamma^{(B)}_{(b,\mathrm{dc})}.
\end{aligned}$$

Decoy methods allow us to restrict out attention to rounds where Alice sent single photons. Thus her Hilbert space is qubit while Bob holds two optical modes. The joint Alice-Bob POVM elements

for the basis b can be constructed via Eqs. (2), (3) and (57) and are given by

$$\begin{aligned}
\Gamma_{(b,b),(\perp)} =& \mathrm{I}_A \otimes \sum_{N_0,N_1=0}^{\infty} (1-d_{b_0})(1-d_{b_1})(1-\eta_{b_0})^{N_0}(1-\eta_{b_1})^{N_1} \,|N_0,N_1\rangle\langle N_0,N_1|_b \\
\Gamma_{(b,b),(\neq)} =& |0\rangle\langle 0|_b \otimes (1-d_{b_0}) \sum_{N_0,N_1=0}^{\infty} (1-\eta_{b_0})^{N_0}(1-(1-d_{b_1})(1-\eta_{b_1})^{N_1}) \,|N_0,N_1\rangle\langle N_0,N_1|_b \\
&+ |1\rangle\langle 1|_b \otimes (1-d_{b_1}) \sum_{N_0,N_1=0}^{\infty} (1-(1-d_{b_0})(1-\eta_{b_0})^{N_0})(1-\eta_{b_1})^{N_1} \,|N_0,N_1\rangle\langle N_0,N_1|_b \\
&+ \mathrm{I}_A \otimes \frac{1}{2}\Gamma^{(B)}_{(b,\mathrm{dc})} \\
\Gamma_{(b,b),(=)} =& |0\rangle\langle 0|_b \otimes (1-d_{b_1}) \sum_{N_0,N_1=0}^{\infty} (1-(1-d_{b_0})(1-\eta_{b_0})^{N_0})(1-\eta_{b_1})^{N_1} \,|N_0,N_1\rangle\langle N_0,N_1|_b \\
&+ |1\rangle\langle 1|_b \otimes (1-d_{b_0}) \sum_{N_0,N_1=0}^{\infty} (1-\eta_{b_0})^{N_0}(1-(1-d_{b_1})(1-\eta_{b_1})^{N_1}) \,|N_0,N_1\rangle\langle N_0,N_1|_b \\
&+ \mathrm{I}_A \otimes \frac{1}{2}\Gamma^{(B)}_{(b,\mathrm{dc})},
\end{aligned} \tag{58}$$

where $|0\rangle\langle 0|_b$ on Alice's system is the $|0\rangle$ state encoded in basis b. Note that this is different from the vacuum state $|0,0\rangle\langle 0,0|_b$ on Bob's system, the state with 0 photons in all modes.

In any practical protocol, the detection efficiencies η_{b_i} and dark count rates d_{b_i} cannot be characterized exactly. Therefore, instead of assuming exact knowledge of these parameters, we assume that they are characterized upto some tolerances $\Delta_\eta, \Delta_{\mathrm{dc}}$ given by

$$\begin{aligned}
\eta_{b_i} &\in [\eta_{\mathrm{det}}(1-\Delta_\eta), \eta_{\mathrm{det}}(1+\Delta_\eta)], \\
d_{b_i} &\in [d_{\mathrm{det}}(1-\Delta_{\mathrm{dc}}), d_{\mathrm{det}}(1+\Delta_{\mathrm{dc}})].
\end{aligned} \tag{59}$$

6.4 Computing bounds on δ_1, δ_2

In this subsection, we will compute upper bounds on δ_1, δ_2 by following the recipe in Section 6.1.

6.4.1 Active BB84 detection setup without any hardware modification

In this case the POVMs used by Alice and Bob are exactly given by Eq. (58). We construct the POVMs from Eqs. (54) and (55) in Section G.1. To bound δ_1, δ_2, we use the fact that all POVMs are block-diagonal in the total photon number, and bound the ∞-norm of each block separately. Note that we can always treat the common value of loss in the detectors to be a part of the channel [53, Section III C]. This means that we pull out $(\max_{b,i}\{\eta_{b_i}\})$, and treat it as a part of the channel. (This is equivalent to giving the $\{\tilde{F}, \mathrm{I}-\tilde{F}\}$ measurement to Eve.) This computation of δ_1, δ_2 using the above steps is quite cumbersome, and is explained in Sections G.2 and G.3. Finally, we obtain

$$\begin{aligned}
\delta_1 &\leq \max\left\{\left(1-\frac{1-(1-d_{\mathrm{min}})^2}{1-(1-d_{\mathrm{max}})^2}\right)\frac{d_{\mathrm{max}}(2-d_{\mathrm{min}})}{1-(1-d_{\mathrm{min}})^2}, 4\left|1-\sqrt{1-(1-d_{\mathrm{min}})^2(1-r_\eta)}\right|\right\}, \\
\delta_2 &\leq \max\left\{1-\frac{1-(1-d_{\mathrm{min}})^2}{1-(1-d_{\mathrm{max}})^2}, (1-d_{\mathrm{min}})^2(1-r_\eta)\right\},
\end{aligned} \tag{60}$$

where

$$\begin{aligned}
r_\eta &= \eta_{\mathrm{min}}/\eta_{\mathrm{max}} \\
d_{\mathrm{max}} &= \max\{d_{X_0}, d_{X_1}, d_{Z_0}, d_{Z_1}\} \leq d_{\mathrm{det}}(1+\Delta_{\mathrm{dc}}), \quad \text{and } d_{\mathrm{min}} = \min\{d_{X_0}, d_{X_1}, d_{Z_0}, d_{Z_1}\} \geq d_{\mathrm{det}}(1-\Delta_{\mathrm{dc}}), \\
\eta_{\mathrm{max}} &= \max\{\eta_{X_0}, \eta_{X_1}, \eta_{Z_0}, \eta_{Z_1}\} \leq \eta_{\mathrm{det}}(1+\Delta_\eta), \quad \text{and } \eta_{\mathrm{min}} = \min\{\eta_{X_0}, \eta_{X_1}, \eta_{Z_0}, \eta_{Z_1}\} \geq \eta_{\mathrm{det}}(1-\Delta_\eta).
\end{aligned} \tag{61}$$

Thus, upper bounds on δ_1, δ_2 can be computed using Eq. (60) and the bounds in Eq. (61). It is these bounds that we use to compute key rates.

6.4.2 Random Swapping of 0 and 1 Detectors

In [13] it was argued that random swapping of the 0 and the 1 detector can be used to remove basis-efficiency mismatch for single-photon pulses entering Bob's detectors. Note that this trick *only works for the single-photon subspace*. We will now adapt our analysis to the case where Bob randomly swaps the 0 and the 1 detector.

In the scenario where we randomly swap the 0 and the 1 detectors, we make certain physically motivated assumptions (Eq. (62)) about the detector setup. In particular, we assume that the dark count rate is a property of the detector only. Furthermore, we assume that the basis choice setting does not change the detector parameters. This means that the dark count rate and detection efficiency in both bases is the same (though these can be different for each detector). Thus, we have

$$\begin{aligned} \eta_{X_0} &= \eta_{Z_0} =: \eta_0 \\ \eta_{X_1} &= \eta_{Z_1} =: \eta_1 \\ d_{X_0} &= d_{Z_0} =: d_0 \\ d_{X_1} &= d_{Z_1} =: d_1. \end{aligned} \tag{62}$$

We will see that this indeed allows us to obtain improved results, even though it does not completely remove efficiency mismatch. In particular, the leading order terms in δ_1, δ_2 are improved in the new bounds obtained in Eqs. (64) and (65). Note that our metrics δ_1, δ_2 do not improve unless we make these assumptions. These assumptions are also implicit in the claims presented in Ref. [13].

If the random swapping is implemented with probability p, the Bob's POVM elements are given by

$$\begin{aligned} \Gamma^{(B),(\mathrm{swap})}_{(b,\perp)} &= \sum_{N_0,N_1=0}^{\infty} (1-d_{b_0})(1-d_{b_1}) \left((1-p)(1-\eta_{b_0})^{N_0}(1-\eta_{b_1})^{N_1} + p(1-\eta_{b_1})^{N_0}(1-\eta_{b_0})^{N_1}\right) |N_0,N_1\rangle\langle N_0,N_1|_b \\ \Gamma^{(B),(\mathrm{swap})}_{(b,0)} &= \Big((1-p)(1-d_{b_1}) \sum_{N_0,N_1=0}^{\infty} (1-(1-d_{b_0})(1-\eta_{b_0})^{N_0})(1-\eta_{b_1})^{N_1} \\ &\quad + p(1-d_{b_0}) \sum_{N_0,N_1=0}^{\infty} (1-(1-d_{b_1})(1-\eta_{b_1})^{N_0})(1-\eta_{b_0})^{N_1}\Big) |N_0,N_1\rangle\langle N_0,N_1|_b + \frac{1}{2}\Gamma^{(B)}_{(b,\mathrm{dc})} \\ \Gamma^{(B),(\mathrm{swap})}_{(b,1)} &= \Big((1-p)(1-d_{b_0}) \sum_{N_0,N_1=0}^{\infty} (1-\eta_{b_0})^{N_0}(1-(1-d_{b_1})(1-\eta_{b_1})^{N_1}) \\ &\quad + p(1-d_{b_1}) \sum_{N_0,N_1=0}^{\infty} (1-\eta_{b_1})^{N_0}(1-(1-d_{b_0})(1-\eta_{b_0})^{N_1})\Big) |N_0,N_1\rangle\langle N_0,N_1|_b + \frac{1}{2}\Gamma^{(B)}_{(b,\mathrm{dc})}, \end{aligned} \tag{63}$$

analogously to Eq. (57). Alice and Bob's joint POVM elements can be constructed from Eqs. (2), (3) and (63) analogously to Eq. (58). Therefore we can repeat the calculations for δ_1, δ_2 using the recipe from Section 6.1. We explain these computations in Section H and obtain (for swap probability $p = 1/2$)

$$\begin{aligned} \delta_1 &\leq 4\left(1 - \sqrt{1-(1-d_{\mathrm{mult}})^2\frac{(1-r_\eta)^2}{2}}\right), \\ \delta_2 &\leq (1-d_{\mathrm{mult}})^2\frac{(1-r_\eta)^2}{2}, \end{aligned} \tag{64}$$

where

$$\begin{aligned} d_{\mathrm{mult}} &= 1 - \sqrt{(1-d_0)(1-d_1)} \geq d_{\min}, \\ r_\eta &= \frac{\eta_{\min}}{\eta_{\max}} \geq \frac{1-\Delta_\eta}{1+\Delta_\eta}. \end{aligned} \tag{65}$$

Thus, upper bounds on δ_1, δ_2 in case of random swapping of detectors can be computed using Eq. (64) and the bounds in Eq. (65). We see that these bounds are better than the earlier bounds

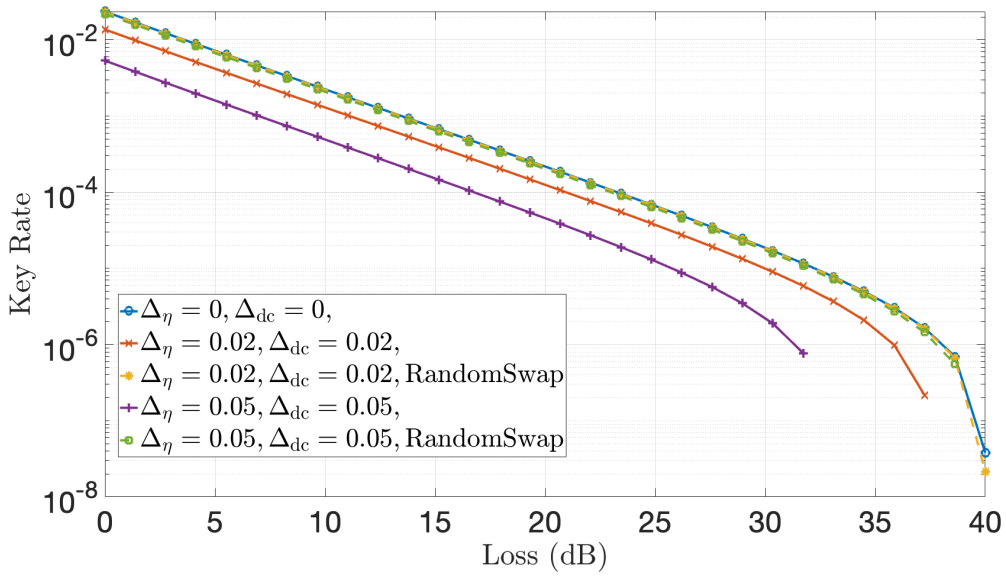


Figure 4: Finite-size key rates in the presence of basis-efficiency mismatch, for the decoy-state BB84 protocol, against loss. We plot key rates for $N_{\text{tot}} = 10^{12}$ number of total signals sent, for various values of $\Delta_\eta, \Delta_{\text{dc}}$. We find that random swapping of the 0 and 1 detectors drastically improves the key rates obtained.

from Eq. (60). On inspecting our calculations from Section H, we find that the zero-photon component of δ_1, δ_2 goes to zero due to $d_X = d_Z$. Furthermore, random swapping in addition to the assumption of $\eta_X = \eta_Z$ leads to the single-photon contribution also being zero. Thus, we are left with the two-photon contribution.

6.5 Plots

We plot finite size key rates for the decoy-state BB84 protocol described in Section 5.1. We choose typical protocol parameters and plot the key rate for the expected observations for a given channel model. For best results, one would optimize over the protocol parameter choices. For all plots, we set the basis choice probabilities to be $p^{(A)}_{(Z)} = p^{(B)}_{(Z)} = 0.5$ and $p^{(A)}_{(X)} = p^{(B)}_{(X)} = 0.5$, and $p_{\text{Z,T}} = 0.05$ (probability of Z basis rounds used for testing). We set the detector parameters to be $\eta_{\text{det}} = 0.7$ and $d_{\text{det}} = 10^{-6}$. We set the misalignment angle θ to be 2°. We set the number of bits used for error-correction to be $\lambda_{\text{EC}}(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_Z) = f_{\text{EC}} n_K h(e^{\text{obs}}_Z)$, where $f_{\text{EC}} = 1.16$ is the error-correction efficiency. The decoy intensities are chosen to be $\mu_1 = 0.9$, $\mu_2 = 0.1$, and $\mu_3 = 0$. Each intensity is chosen with equal probability. We set $\varepsilon_{\text{AT-a}} = \varepsilon_{\text{AT-b}} = \varepsilon_{\text{AT-c}} = \varepsilon_{\text{AT-d}} = \varepsilon_{\text{EV}} = \varepsilon_{\text{PA}} = 10^{-12}$. This leads to a value of $\varepsilon_{\text{AT}} = \sqrt{12} \times 10^{-12}$. The overall security parameter is then given by $(2\sqrt{12} + 2)10^{-12}$. Due to machine precision issues arising from small values of $\varepsilon^2_{\text{AT}}$, we use Hoeffdings inequality to bound γ_{bin} (Eq. (27)) instead of using the cumulative binomial distribution (which is tighter).

1. In Fig. 4, we plot the finite size key rate against loss for various values of detector characterizations $\Delta_\eta, \Delta_{\text{dc}}$ for $n_{\text{total}} = 10^{12}$ number of total signals. For $\Delta_\eta = \Delta_{\text{dc}} = 0$, we have $\delta_1 = \delta_2 = 0$. Therefore the phase error rate bound from Eq. (34) reduces to the scenario where the basis-independent loss assumption is satisfied (Eq. (14)). For non-zero values of $\Delta_\eta, \Delta_{\text{dc}}$, the key rate is reduced. This is mostly due to the increase in the bound for the phase error rate from Eq. (34) from δ_1. We find that random swapping leads to a dramatic improvement in performance.

2. In Fig. 5, we plot the finite size key rate against loss for various values of total signals sent. We set $\Delta_\eta = \Delta_{\text{dc}} = 0.05$. We find that we get close to asymptotic key rates already at $N_{\text{tot}} = 10^{12}$ signals sent.

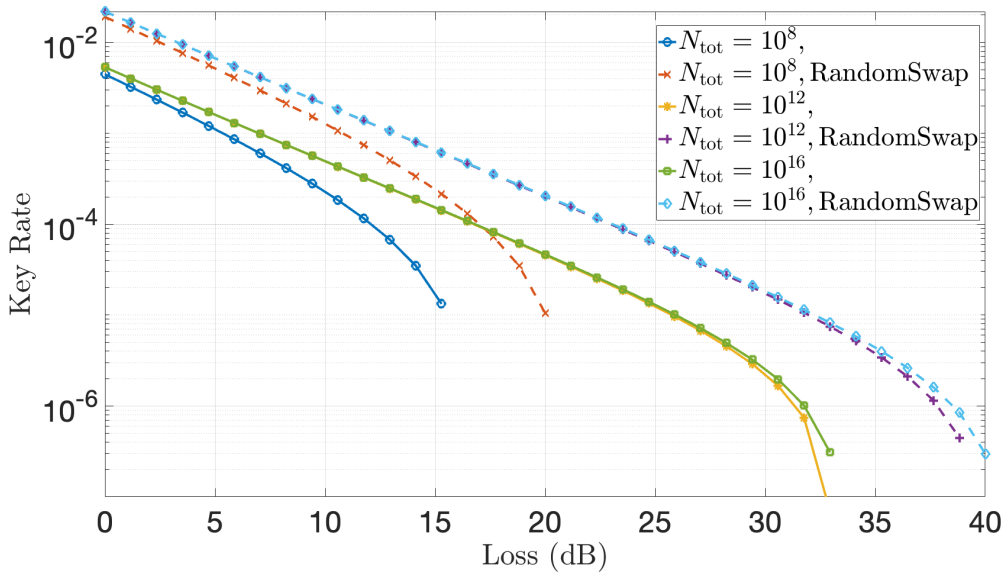


Figure 5: Finite-size key rates in the presence of basis-efficiency mismatch, for the decoy-state BB84 protocol against loss. We plot key rates for various values of total number of signals sent (N_{tot}), for $\Delta_\eta = \Delta_{\text{dc}} = 0.05$.

3. In Fig. 6, we plot the finite size key rate against detector characterization parameters $\Delta_\eta, \Delta_{\text{dc}}$. We find that our methods can tolerate a significant amount of error in detector characterization. In fact, with random swapping of detectors, we get positive key rate for $N_{\text{tot}} = 10^{12}$ signals sent for $\Delta_\eta, \Delta_{\text{dc}}$ upto 0.35.

4. In Fig. 7, we plot the finite size key rate against both detector characterization parameters $\Delta_\eta, \Delta_{\text{dc}}$ independently. We find that both the parameters $\Delta_\eta, \Delta_{\text{dc}}$ lead to comparable penalties in the key rate, although Δ_{dc} penalizes the key rate less than Δ_η. Note that the values for δ_1, δ_2 also depend on the dark count rate d_{det}.

We end this this section by considering a scenario where the detector behavior is independent (but not identical) in each round. In this case each round has a well-defined POVM that is independent of those in other rounds, i.e the POVM is tensor product with other rounds. Here we simply note that all the statistical claims used in our phase error estimation proofs (from Section C.2) remain true even if the POVM measurements are independent (but not IID). We comment on this and restate some of our lemmas for independent (but not identical) measurements in Section C.3. Moreover the Serfling statement (Lemma 2) does not assume any IID property of the input string. Thus, our bounds on the phase error rate remain unchanged as long as δ_1, δ_2 can be bounded for the independent POVMs in each round. Such a scenario is of practical importance, as detection setups are never perfectly IID [54, Fig. 3(a)]. Another important practical consideration is that of correlated detectors, which we now discuss in the next section.

7 Application to Correlated effects

We now turn our attention to detectors exhibiting correlated behavior across the rounds. We begin by formalizing our model for such detectors. Let the outcome of round i for Bob be denoted by k_i, and define k_i^j as the sequence of outcomes from round i to round j ($i \leq j$). Recall that $\perp$ corresponds to the no-detect outcome. Correlated effects such as afterpulsing and detector dead times can be modeled by allowing the POVM used in later rounds to depend on the outcome — in particular, detection events — of previous rounds. This is the scenario we are interested in. More formally, in the ith round, the POVM used for the measurement is given by $\{\Gamma_{k_i}^{(k_{i-l_c}^{i-1})}\}$, where l_c denotes the correlation length. Note that l_c here denotes the correlation length in units of the time

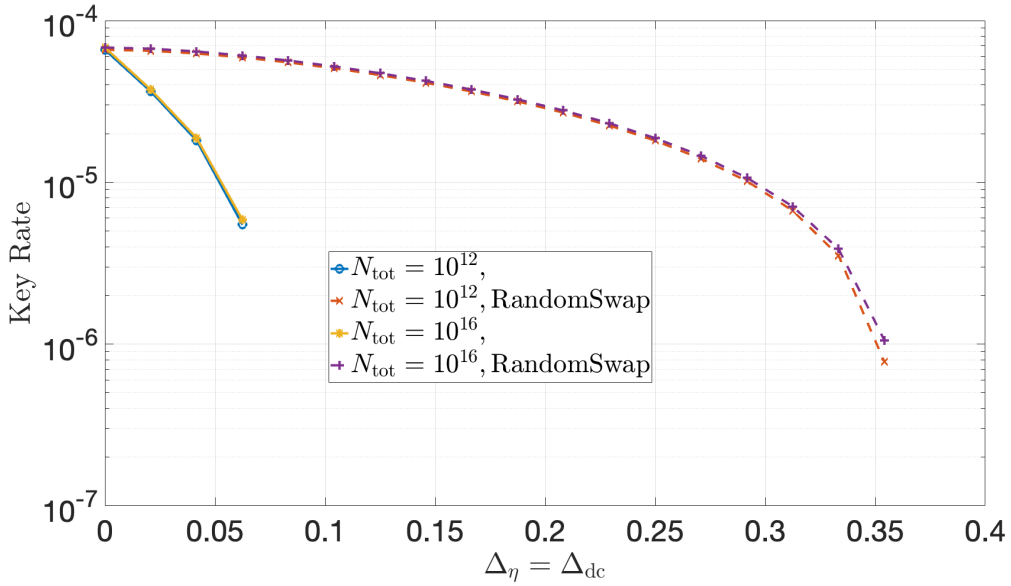


Figure 6: Finite-size key rates in the presence of basis-efficiency mismatch, for the decoy-state BB84 protocol against detector characterization parameters $\Delta_\eta, \Delta_{\mathrm{dc}}$. We plot key rates for a channel with 25dB loss.

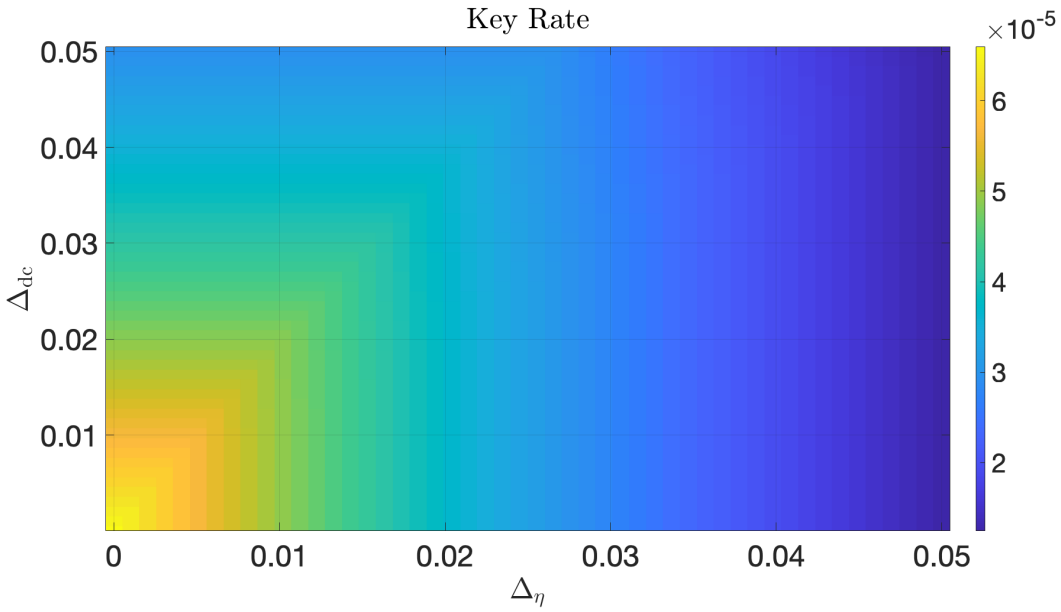


Figure 7: Finite-size key rates for various values of $\Delta_\eta, \Delta_{\mathrm{dc}}$ for the decoy-state BB84 protocol, for $N_{\mathrm{tot}} = 10^{12}$ and 25dB loss. We find that both $\Delta_\eta, \Delta_{\mathrm{dc}}$ have comparable impact on the keyrate, although Δ_{dc} penalizes the key rate less than Δ_η. The above plot is interpolated from key rate calculations of 2500 points, and the detectors are not swapped randomly.

slots (i.e, the unit is the time between successive measurements in the QKD protocol). We use the convention that when all $k_{i-l_c}^{i-1} = \perp s$, then the superscript can be omitted.

Our approach involves a protocol modification in which Alice and Bob retain only those rounds where previous l_c rounds involved only no-click events. All other rounds are 'rejected', i.e thrown away. In our terminology, a round can be rejected in this manner (due to the specific postprocessing described above), but may also be discarded later based on its detection outcome - for instance, if it results in a no-detection event. The idea is that after this postprocessing, the remaining rounds can be thought of as all being measured using uncorrelated POVM $\{\Gamma_{k_i}\}$.

The key idea is to introduce a generalized filtering step (analogous to $\tilde{F}$ in the round-by-round case) that performs the minimum amount of measurements necessary, and uses the outcomes to reject rounds based on the above postprocessing. Once the rounds to be rejected are fixed, the remaining rounds can be measured fully using uncorrelated POVMs, and the analysis on *these* rounds can follow the same approach as the usual EUR analysis.

However, note that the postprocessing described above depends on the detection events, which in turn depend on the choice of basis, and thus can only be determined *after* basis choice. Thus, in general, a basis choice needs to be made *before* rounds can be rejected. This is the core difficulty in proving security under detector correlations within the EUR framework, as the EUR statement must be applied to the state *before* choosing the basis.

We can now present a two-step proof sketch to address the above issue (we elaborate on each step in later subsections):

1. Assuming the detectors have no loss or dark counts, the rejection step can be performed in a basis-independent manner (on the rounds which will not be rejected). Thus, the EUR statement can be applied to those rounds by completing the measurements later. We explicitly construct this procedure in Section 7.1, and show that is rejects the correct rounds (see Lemma 5). Note that here we consider a setting in which the detectors themselves have no intrinsic loss or dark counts, i.e., they are perfect in the absence of correlated effects arising from clicks in previous rounds. However, the detectors suffer from afterpulsing and dead times due to correlated effects.

2. We lift the assumption (of no loss and no dark counts) made in the first step above using techniques from Ref. [55]. Intuitively, Ref. [55] allows one to incorporate the effects of basis-dependent dark counts and efficiencies at some cost (to be discussed in Section 7.2). Thus, this step can be done first, reducing the problem to the analysis described in the earlier step.

7.1 Perfect correlated detectors

The intuition behind the first step relies on the following two observations. First, detections in the rounds that will not be rejected can be inferred from the photon number of the incoming state, independent of basis choice. This is because the previous rounds have had no clicks, so the POVM used in the current is the uncorrelated, perfect one. Moreover, due to the block-diagonal nature of the POVMs, this photon number measurement does not affect the measurement statistics. Second, the EUR statement is not used on the rounds that are rejected. Thus, we are allowed to complete the measurement on these rounds. This can be formalized in the following lemma.

Lemma 5. Consider the state ρ_{Q^n}, and let the ith subsystem be measured using POVM $\{\Gamma_{k_i}^{(k_{i-l_c}^{i-1})}\}$, where k_i denotes the outcome of the ith measurement, and $k_{i-l_c}^{i-1}$ denotes the string of outcomes in the previous l_c rounds. Suppose that $\{\Gamma_{k_i}\}$ (corresponding to $k_{i-l_c}^{i-1} = \perp s$) is such that it can be described by a two-step measurement, where the first measurement $\{\tilde{F}, \mathrm{I} - \tilde{F}\}$ determines the detect vs no-detect, followed by a second step measurement (see Fig. 8). Consider the state obtained after rejecting all rounds i for which a detection occurred in the previous l_c rounds. Then this state can be obtained via a procedure that only performs the $\{\tilde{F}, \mathrm{I} - \tilde{F}\}$ measurements on the rounds that are not rejected.

Proof. For simplicity, we assume a correlation length l_c of 1. The extension to larger, finite correlation lengths is straightforward. We will prove the required claim by explicit construction of the procedure. We will prove it sequentially, from round 1 to round n.

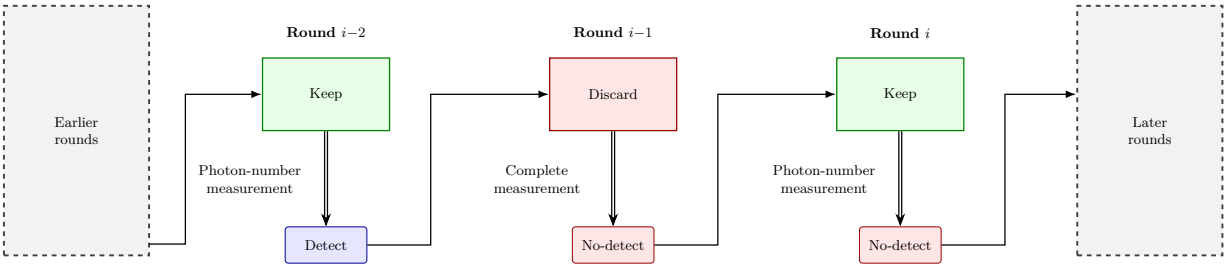


Figure 8: Illustration of the process to determine the rounds that will be rejected based on prior detection events. The rounds that are not rejected are only measured using $\{\tilde{F}, \mathrm{I} - \tilde{F}\}$, which determines the detect vs no-detect outcome. They will have the rest of the measurement, including basis choice, completed at a later stage. The rounds that are rejected have their entire measurements completed in order to determine the detection event.

First note that round 1 will never be rejected. The $\{\tilde{F}, \mathrm{I} - \tilde{F}\}$ measurement in round 1 directly tells us whether or not the round will result in a detection event. Thus, this tells us whether or not the next round ($i = 2$) will be rejected. (Note that this measurement was performed without choosing a measurement basis for round 1.)

For round $i \geq 3$, assume rounds 1 to $i-1$ already have definite reject/no-reject tags, with only the $\{\tilde{F}, \mathrm{I} - \tilde{F}\}$ measurement being performed on the rounds that are not rejected. Then, the round i can be given the correct reject/no-reject tag as follows.

1. To determine whether round i should be kept, check the reject/no-reject tag of round $i - 1$ (which is guaranteed to be correct).

2. If round $i - 1$ is to be rejected, complete the measurement on it. This determines whether or not there is a detection event in this round, which inturn determines whether or not round i will be rejected.

3. If round $i - 1$ is not rejected, then round $i - 2$ must have had no detection (since otherwise the round $i - 1$ would be rejected). This means that the POVM to be used in round $i - 1$ is the uncorrelated one ($\{\Gamma_{k_{i-1}}\}$). Thus, measuring $\{\tilde{F}, \mathrm{I} - \tilde{F}\}$ directly tells us whether or not round $i - 1$ will result in a detection event. This, in turn, determines whether or not round i will be rejected.

By construction, the above procedure only implements the $\{\tilde{F}, \mathrm{I} - \tilde{F}\}$ on the rounds that are not rejected, and results in the correct rounds being rejected. This concludes our proof.

□

7.2 Reduction to perfect correlated detectors

As mentioned earlier, the applicability of Lemma 5 crucially relies on the fact that the detectors are perfect threshold detectors – except for correlations that one detect event might trigger other detect events within the correlation length. However, as argued in the rest of this paper, this is not a practical assumption. To resolve this issue, we use the results of Ref. [55].

Ref. [55] constructs a basis-choice independent reduction from a detection setup with detectors with different dark counts and loss, to a detection setup with perfect detectors. It shows that the imperfect detection setup can be treated as a basis-choice independent channel (similar to the basis-independent filter $\tilde{F}$) followed by the perfect detection setup. To do this, it crucially relies on the flag-state squasher [14]. The intuition is that the flag-state squasher makes it possible to 'give' Eve full information about multi-photon signals by introducing a classical flag space. Crucially, this flag space can also then be used to transfer imperfections such as loss and dark counts to Eve. This is argued formally in [55, Theorem 1 and 2].

The main open task in our approach outlined in this section is the use of the flag-state squasher in an EUR-based security proof. In the typical usage of the flag-state squasher, one considers a single round state, and the weight of the state in the flag space is bounded through suitable methods to prevent trivial results (since the entire flagged state is revealed to Eve). In the EUR context,

there no single round state. Instead, the natural alternative is to instead bound the *number* of rounds in the flag space. We believe that the usual methods of bounding the weight of the state along with suitable concentration inequalities will suffice for this task. However, we emphasize that in this work, we provide only a sketch of the proof for handling correlated detectors, leaving a detailed analysis to future work — a non-trivial task. In the next section, we shift our focus to detector side-channels, and in particular, we will see how our methods naturally address certain detector side-channels as a by-product.

8 Detector Side-Channels

The analysis presented so far assumes that the detector behavior, while possibly varying between rounds or exhibiting correlations, is described by a single mode characterized by bounded loss and dark count rates η_{b_i} and d_{b_i}, as specified in Eq. (59). Thus, we have presented an analysis of Case 2 from Section 1. This analysis allows us to drastically reduce the requirements on device characterization: the proof technique is now robust to imperfect characterization. However, physical implementations of QKD protocols are vulnerable to side-channel attacks where Eve can control, to a limited extent, the POVMs used. For example, by controlling the frequency, spatial mode [20, 56] or arrival time [21] of the light, Eve can partially choose the detector efficiencies and induce a suitable basis-efficiency mismatch. This is the scenario described by Case 3 from Section 1.

While our proof technique advances the theory to the point where this case can be handled in principle, a complete analysis first requires the physical modeling of multi-mode detectors, which remains an open problem. In this section, we outline how the results of this work can be applied to a simple multi-mode model.

We expand our detector model (and Bob's Hilbert space) to account for spatio-temporal modes [14] as

$$\Gamma^{\text{multi}}_{(b_A,b_B),(k)} = \bigoplus_{\mathbf{d}} \Gamma_{(b_A,b_B),(k)}(\{\eta_{b_i}(\mathbf{d}), d_{b_i}(\mathbf{d})\}), \tag{66}$$

where $\mathbf{d}$ denotes the spatio-temporal mode, and $\Gamma_{(b_A,b_B),(k)}(\{\eta_{b_i}(\mathbf{d}), d_{b_i}(\mathbf{d})\})$ denotes the single-mode POVM element corresponding to that mode, and is given by Eq. (58). The multi-mode detector has loss $\eta_{b_i}(\mathbf{d})$ for this mode, and a dark count rate of $d_{b_i}(\mathbf{d})$.

The block-diagonal structure with respect to $\mathbf{d}$ in the above equation reflects the fact that our model assumes no interference between any pair of spatio-temporal modes during the measurement process. In particular, it captures the possibility that an adversary may exploit different times-of-arrival, frequencies, or angles of incidence to attack the system, provided that each instance corresponds to a definite spatio-temporal mode and no coherent superpositions across modes, or multi-excitation states that simultaneously occupy several modes are used. Even with these limitations, the model protects against a wide range of known classical side-channel attacks. For instance, the time-shift attack [18, 21] is fully captured within this model, as it simply corresponds to Eve selecting different times-of-arrival to exploit the time-dependent efficiency mismatch of the gated detectors. Thus, the block-diagonal model represents a first step toward a more complete analysis of realistic side-channels. This perspective also captures other potential attack strategies, such as modifying the temperature of the detection setup.

Remark 15. We stress that our results in this subsection should be interpreted within the context of this model, and may not accurately describe the physical reality of multi-mode detectors. Nevertheless, while we only consider models of the above form in this work, our proof provides a framework to accommodate more complicated models of multi-mode detectors with off-diagonal blocks, as long as one can suitably bound δ_1, δ_2. In general, this would require a model of the detectors, and characterization of the detectors over all the modes. For examples of such attempts to experimentally characterize all the modes, see Ref. [20, 56].

Due to the block-diagonal structure of the above POVM element Eq. (66), and the fact that δ_1, δ_2 are ∞-norms which can be computed on each block-diagonal part separately, it is straightforward to see that our computation of δ_1, δ_2 is directly applicable to the above scenario. To see this, note that our metrics are obtained by first constructing POVMs corresponding to a multi-step

measurement process, as outlined in Section 6.1. This construction preserves the block-diagonal structure of Eq. (66). Thus, if $\delta_1(\{\eta_{b_i}(\mathbf{d}), d_{b_i}(\mathbf{d})\}), \delta_2(\{\eta_{b_i}(\mathbf{d}), d_{b_i}(\mathbf{d})\})$ are the values of these metrics computed according to Eq. (56), for the appropriate single-mode POVMs, then the metrics for the multi-mode case are given by

$$\begin{aligned} \delta_1^{\text{multi}} &= \max_{\mathbf{d}} \delta_1(\{\eta_{b_i}(\mathbf{d}), d_{b_i}(\mathbf{d})\}), \\ \delta_2^{\text{multi}} &= \max_{\mathbf{d}} \delta_2(\{\eta_{b_i}(\mathbf{d}), d_{b_i}(\mathbf{d})\}). \end{aligned} \tag{67}$$

If the values of $\{\eta_{b_i}(\mathbf{d}), d_{b_i}(\mathbf{d})\}$ are characterized and satisfy Eq. (59) for all $\mathbf{d}$, then Eq. (67) is exactly the same as the computation as in Step (5) of Section 6.1 (which corresponds to computing δ_1, δ_2 for Case 2 from Section 1).

This means that the recipe from Section 6.1, and the computed key rates from Section 6.5 are valid for the scenario where Eve can choose the value of η_{b_i}, d_{b_i} in the specified ranges (Eq. (59)), via some extra spatio-temporal modes. Most importantly, our analysis does not depend on the *number* of such spatio-temporal modes. Thus, we are able to address scenarios where Eve has an arbitrary number of spatio-temporal modes, to induce (a bounded amount of) basis-efficiency mismatch in the detector.

Remark 16. As discussed above, our methods are such that allowing Eve to choose the detector parameters within the characterized range yields the same key rate as having fixed detector parameters that are characterized within the same range. However, this observation need not be fundamental, and may be a consequence of the proof technique used in this work. This is because intuitively, we expect scenarios where Eve cannot choose the detector parameters (from within their respective ranges), to lead to higher key rates than scenarios where she can, since she is strictly stronger in the latter scenario. Nevertheless, while we do not know of a physical mechanism by which Eve can choose dark count rates, we allow Eve to choose them along with the detection efficiency.

We have picked this model for its theoretical simplicity. However, more realistic models such as the one introduced in [13, Section 3] can also be analysed with the results in this work. In that case, the computation of δ_1 and δ_2 would constitute a more involved version of our current computations described in Section G. Specifically, Eq. (121) would need to be modified with a different choice of operator P. We note that the basis dependent filters for this model are still block-diagonal in the total number of photons n across all modes. Moreover, as n increases, the filtering operators approach the identity operator (since the probability of detect approaches 1). Thus, we expect δ_1 and δ_2 to depend on the $n \leq 1$ blocks. If this monotonicity can be rigorously proven, then the $n \leq 1$ block contributions to δ_1 and δ_2 can even be computed numerically.

Finally we note that this work does not apply to *all* detector side-channels. For instance, our model does not fit Trojan horse attacks [57]. Moreover, some blinding attacks on detectors [58] lead to complete knowledge of Bob's detection events to Eve. In this case, our methods naturally lead to trivial key rates, since no key generation is possible.

9 Summary and Discussion

In this work, we presented a finite-size security proof of the decoy-state BB84 protocol in the presence of imperfectly characterized and (bounded) adversary controlled basis-efficiency mismatch. Thus, we addressed a longstanding assumption made in security proofs for such protocols within the EUR and phase error correction frameworks. Before this work, proofs within these frameworks were not stable, and would be invalidated by infinitesimal amounts of basis-efficiency mismatch (This problem does not arise in MDI-QKD, and is not resolved by this work for entanglement-based protocols). Since our methods permit (bounded) adversarial control over the efficiency mismatch, we also develop a framework to address an important class of detector side-channels, which has remained unresolved in existing security proof approaches for standard QKD.

We also fixed several technical issues in the security analysis of decoy-state QKD within the EUR framework. We applied our results to the decoy-state BB84 protocol, demonstrating practical key rates in the finite-size regime even in the presence of basis-efficiency mismatch. We also investigate

quantitatively, the effect of methods such as random swapping of detectors, to reduce efficiency mismatch. Taken together, these results are a significant step towards protocol security of the EUR proof technique, and the implementation security of QKD using trusted detection setups.

Moreover, although the rigorous results we obtain for multi-mode detectors depend on a specific model, we expect this framework to be adapted to more realistic models with subsequent work. For computing key rates based on our results, suitable bounds on δ_1, δ_2 are required. While our current analysis relies on some simplifications to obtain these bounds, they can likely be improved. Finally, examining a wider spectrum of detector imperfections – well characterized by state-of-the-art experimental methods – would further broaden the applicability of our results. Such an endeavor would require close collaboration with experimentalists to refine the characterization of imperfections, as well as theoretical advancements to extend the framework to encompass a wider class of side channels.

We note that results from this work have already been used for subsequent work on QKD security analysis. For instance, in this work, we only sketch a possible approach to handling correlated detectors - an open problem on which there has been little progress so far. Ref. [59] obtains rigorous results for correlated detector effects within phase error based frameworks. It follows the same essential idea presented here, but incorporates some modifications necessary for a fully rigorous analysis. Another natural extension is to integrate our methods with established methods for addressing source imperfections [7–9]. Such a combination would lead to a security proof robust to both source and detector imperfections. Such a result has also been recently obtained in Ref. [60]. Another avenue is applying these methods to passive detection setups, where the basis-efficiency mismatch assumption translates to an assumption of a perfectly balanced beam splitter and identical detectors. Such a result has also been recently obtained in Refs. [59, 61].

References

[1] Marco Tomamichel and Renato Renner. "Uncertainty Relation for Smooth Entropies". Physical Review Letters **106**, 110506 (2011).

[2] Marco Tomamichel and Anthony Leverrier. "A largely self-contained and complete security proof for quantum key distribution". Quantum **1**, 1–38 (2017). arXiv:1506.08458.

[3] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. "Tight finite-key analysis for quantum cryptography". Nature Communications **3**, 634 (2012).

[4] Devashish Tupkary, Ernest Y. Z. Tan, Shlok Nahar, Lars Kamin, and Norbert Lütkenhaus. "QKD security proofs for decoy-state BB84: protocol variations, proof techniques, gaps and limitations" (2025). arXiv:2502.10340.

[5] Masato Koashi. "Simple security proof of quantum key distribution via uncertainty principle" (2005). arXiv:quant-ph/0505108.

[6] M. Koashi. "Simple security proof of quantum key distribution based on complementarity". New Journal of Physics **11**, 045018 (2009).

[7] Margarida Pereira, Guillermo Currás-Lorenzo, Álvaro Navarrete, Akihiro Mizutani, Go Kato, Marcos Curty, and Kiyoshi Tamaki. "Modified BB84 quantum key distribution protocol robust to source imperfections". Physical Review Research **5**, 023065 (2023).

[8] Kiyoshi Tamaki, Marcos Curty, Go Kato, Hoi-Kwong Lo, and Koji Azuma. "Loss-tolerant quantum cryptography with imperfect sources". Physical Review A **90**, 052314 (2014).

[9] Guillermo Currás-Lorenzo, Margarida Pereira, Go Kato, Marcos Curty, and Kiyoshi Tamaki. "Security framework for quantum key distribution with imperfect sources". Optica Quantum **3**, 525 (2025).

[10] Víctor Zapatero, Álvaro Navarrete, and Marcos Curty. "Implementation security in quantum key distribution". Advanced Quantum Technologies **8**, 2300380 (2025). arXiv:https://advanced.onlinelibrary.wiley.com/doi/pdf/10.1002/qute.202300380.

[11] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. "Measurement-device-independent quantum key distribution". Physical Review Letters **108**, 130503 (2012). arXiv:1109.1473.

[12] L. Lydersen and J. Skaar. "Security of quantum key distribution with bit and basis dependent detector flaws" (2010). arXiv:0807.0767.

[13] Chi-Hang Fred Fung, Kiyoshi Tamaki, Bing Qi, Hoi-Kwong Lo, and Xiongfeng Ma. "Security proof of quantum key distribution with detection efficiency mismatch". Quantum Information and Computation **9**, 131–165 (2009). arXiv:0802.3788.

[14] Yanbao Zhang, Patrick J. Coles, Adam Winick, Jie Lin, and Norbert Lütkenhaus. "Security proof of practical quantum key distribution with detection-efficiency mismatch". Physical Review Research **3**, 013076 (2021). arXiv:2004.04383.

[15] M. K. Bochkov and A. S. Trushechkin. "Security of quantum key distribution with detection-efficiency mismatch in the single-photon case: Tight bounds". Physical Review A **99**, 032308 (2019).

[16] Anton Trushechkin. "Security of quantum key distribution with detection-efficiency mismatch in the multiphoton case". Quantum **6**, 771 (2022).

[17] Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. "Full-field implementation of a perfect eavesdropper on a quantum cryptography system". Nature Communications **2**, 349 (2011).

[18] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. "Effects of detector efficiency mismatch on security of quantum cryptosystems". Physical Review A **74**, 022313 (2006). arXiv:quant-ph/0511032.

[19] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. "Hacking commercial quantum cryptography systems by tailored bright illumination". Nature Photonics **4**, 686–689 (2010).

[20] Shihan Sajeed, Poompong Chaiwongkhot, Jean-Philippe Bourgoin, Thomas Jennewein, Norbert Lütkenhaus, and Vadim Makarov. "Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch". Physical Review A **91**, 062301 (2015). arXiv:1502.02785.

[21] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. "Time-shift attack in practical quantum cryptosystems". Quantum Info. Comput. **7**, 7382 (2007). arXiv:quant-ph/0512080.

[22] ETSI. "Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems" (2016).

[23] Toyohiro Tsurumaru. "Equivalence of three classical algorithms with quantum side information: Privacy amplification, error correction, and data compression". IEEE Transactions on Information Theory **68**, 1016–1031 (2022). arXiv:2009.08823.

[24] Toyohiro Tsurumaru. "Leftover hashing from quantum error correction: Unifying the two approaches to the security proof of quantum key distribution". IEEE Transactions on Information Theory **66**, 3465–3484 (2020). arXiv:1809.05479.

[25] Christopher Portmann and Renato Renner. "Security in quantum cryptography". Reviews of Modern Physics **94**, 025008 (2022).

[26] Michael Ben-Or, Michał Horodecki, Debbie W. Leung, Dominic Mayers, and Jonathan Oppenheim. "The universal composable security of quantum key distribution". In Proceedings of the Second International Conference on Theory of Cryptography. Pages 386–406. TCC'05Berlin, Heidelberg (2005). Springer-Verlag.

[27] Devashish Tupkary, Ernest Y.-Z. Tan, and Norbert Lütkenhaus. "Security proof for variable-length quantum key distribution". Phys. Rev. Res. **6**, 023002 (2024).

[28] Matthias Christandl, Robert König, and Renato Renner. "Postselection technique for quantum channels with applications to quantum cryptography". Physical Review Letters **102**, 1–4 (2009). arXiv:0809.3019.

[29] Shlok Nahar, Devashish Tupkary, Yuming Zhao, Norbert Lütkenhaus, and Ernest Y.-Z. Tan. "Postselection technique for optical quantum key distribution with improved de finetti reductions". PRX Quantum **5**, 040315 (2024).

[30] Masahito Hayashi and Toyohiro Tsurumaru. "Concise and tight security analysis of the Bennett–Brassard 1984 protocol with finite key lengths". New Journal of Physics **14**, 093014 (2012).

[31] Shun Kawakami. "Security of Quantum Key Distribution with Weak Coherent Pulses". PhD thesis. University of Tokyo. (2018). url: `https://repository.dl.itc.u-tokyo.ac.jp/records/50621`.

[32] Guillermo Currás-Lorenzo, Álvaro Navarrete, Koji Azuma, Go Kato, Marcos Curty, and Mohsen Razavi. "Tight finite-key security for twin-field quantum key distribution". npj Quantum Information **7**, 1–9 (2021).
[33] Øystein Marøy, Lars Lydersen, and Johannes Skaar. "Security of quantum key distribution with arbitrary individual imperfections". Physical Review A**82** (2010).
[34] Alessandro Marcomini, Akihiro Mizutani, Fadri Grnenfelder, Marcos Curty, and Kiyoshi Tamaki. "Loss-tolerant quantum key distribution with detection efficiency mismatch". Quantum Science and Technology **10**, 035002 (2025).
[35] Charles Ci Wen Lim, Marcos Curty, Nino Walenta, Feihu Xu, and Hugo Zbinden. "Concise security bounds for practical decoy-state quantum key distribution". Physical Review A **89**, 022307 (2014).
[36] Tobias Moroder, Marcos Curty, and Norbert Lütkenhaus. "Detector decoy quantum key distribution". New Journal of Physics **11**, 045008 (2009).
[37] Adam Winick, Norbert Lütkenhaus, and Patrick J. Coles. "Reliable numerical key rates for quantum key distribution". Quantum **2**, 77 (2018). arXiv:1710.05511.
[38] Federico Grasselli, Giovanni Chesi, Nathan Walk, Hermann Kampermann, Adam Widomski, Maciej Ogrodnik, Michał Karpiński, Chiara Macchiavello, Dagmar Bruß, and Nikolai Wyderka. "Quantum key distribution with basis-dependent detection probability". Phys. Rev. Appl. **23**, 044011 (2025).
[39] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus. "Entanglement as a Precondition for Secure Quantum Key Distribution". Physical Review Letters **92**, 217903 (2004).
[40] Agnes Ferenczi and Norbert Lütkenhaus. "Symmetries in Quantum Key Distribution and the Connection between Optimal Attacks and Optimal Cloning". Physical Review APages 1–19 (2011). arXiv:1112.3396.
[41] R. J. Serfling. "Probability Inequalities for the Sum in Sampling without Replacement". The Annals of Statistics **2**, 39 – 48 (1974).
[42] Won-Young Hwang. "Quantum Key Distribution with High Loss: Toward Global Secure Communication". Physical Review Letters **91**, 057901 (2003).
[43] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. "Decoy State Quantum Key Distribution". Physical Review Letters **94**, 230504 (2005).
[44] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. "Practical decoy state for quantum key distribution". Physical Review A **72**, 012326 (2005).
[45] Masahito Hayashi and Ryota Nakayama. "Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths". New Journal of Physics **16**, 063009 (2014). arXiv:1302.4139.
[46] Marcos Curty, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi-Kwong Lo. "Finite-key analysis for measurement-device-independent quantum key distribution". Nature Communications **5**, 3732 (2014).
[47] Corsin Pfister, Norbert Lütkenhaus, Stephanie Wehner, and Patrick J. Coles. "Sifting attacks in finite-size quantum key distribution". New Journal of Physics **18**, 053001 (2016). arXiv:1506.07502.
[48] Kiyoshi Tamaki, Hoi-Kwong Lo, Akihiro Mizutani, Go Kato, Charles Ci Wen Lim, Koji Azuma, and Marcos Curty. "Security of quantum key distribution with iterative sifting". Quantum Science and Technology **3**, 014002 (2018). arXiv:1610.06499.
[49] Chi-Hang Fred Fung, Xiongfeng Ma, and H. F. Chau. "Practical issues in quantum-key-distribution postprocessing". Physical Review A **81**, 012318 (2010).
[50] Jerome Wiesemann, Jan Krause, Devashish Tupkary, Norbert Lütkenhaus, Davide Rusca, and Nino Walenta. "A consolidated and accessible security proof for finite-size decoy-state quantum key distribution" (2024). arXiv:2405.16578.
[51] Davide Rusca, Alberto Boaron, Fadri Grünenfelder, Anthony Martin, and Hugo Zbinden. "Finite-key analysis on the 1-decoy state QKD protocol" (2018). arXiv:1801.03443.
[52] Lars Kamin and Norbert Lütkenhaus. "Improved decoy-state and flag-state squashing methods". Phys. Rev. Res. **6**, 043223 (2024).
[53] Yanbao Zhang and Norbert Lütkenhaus. "Entanglement verification with detection-efficiency mismatch". Physical Review A **95**, 042319 (2017).

[54] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields. "High speed prototype quantum key distribution system and long term field trial". Opt. Express **23**, 7583–7592 (2015).
[55] Shlok Nahar, Devashish Tupkary, and Norbert Lütkenhaus. "Imperfect detectors for adversarial tasks with applications to quantum key distribution" (2025). arXiv:2503.06328.
[56] Markus Rau, Tobias Vogl, Giacomo Corrielli, Gwenaelle Vest, Lukas Fuchs, Sebastian Nauerth, and Harald Weinfurter. "Spatial mode side channels in free-space qkd implementations". IEEE Journal of Selected Topics in Quantum Electronics **21**, 187–191 (2015).
[57] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. "Trojan-horse attacks on quantum-key-distribution systems". Physical Review A**73** (2006).
[58] Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. "Full-field implementation of a perfect eavesdropper on a quantum cryptography system". Nature Communications**2** (2011).
[59] Zhiyao Wang, Devashish Tupkary, and Shlok Nahar. "Phase error estimation for passive detection setups with imperfections and memory effects" (2025). arXiv:2508.21486.
[60] Guillermo Currs-Lorenzo, Margarida Pereira, Shlok Nahar, and Devashish Tupkary. "Security of quantum key distribution with source and detector imperfections through phase-error estimation" (2025). arXiv:2507.03549.
[61] Akihiro Mizutani, Shun Kawakami, and Go Kato. "Finite-key security analysis of the decoy-state bb84 qkd with passive measurement". Quantum Science and Technology **11**, 015010 (2025).
[62] Marco Tomamichel. "Quantum Information Processing with Finite Resources". Volume 5 of SpringerBriefs in Mathematical Physics. Springer International Publishing. Cham (2016).
[63] Marco Tomamichel. "A Framework for Non-Asymptotic Quantum Information Theory" (2013). arXiv:1203.2142.
[64] Wassily Hoeffding. "Probability Inequalities for Sums of Bounded Random Variables". Journal of the American Statistical Association **58**, 13–30 (1963).

Author Contributions

This project was formulated and led by DT. DT is responsible for the contributions in Sections B, 3, 5 and F. DT and SN are responsible for the contributions in Sections 4 and 6 to 8. The proofs of the lemmas in Section C.2 are due to PS. NL contributed to supervision and general directions for the project.

Code Availablility

The code used in this paper is available at https://openqkdsecurity.wordpress.com/repositories-for-publications/.

Acknowledgements

We thank Victor Zapatero, Margarida Pereira, and Guillermo Currs-Lorenzo for useful discussions on the phase error correction framework and the EUR approach to QKD security proofs, and for providing helpful comments on this manuscript. We thank Ernest Tan for useful discussions that led to the variable-length security proof in this work. We thank Ashutosh Marwah for some helpful comments on our random sampling arguments. We thank Masato Koashi, and Antia Lamas-Linares for helpful discussions on the detector model used in this work. We thank John Burniston for help with code. We thank Federico Grasselli for detailed feedback on early versions of this work. This work was funded by the NSERC Discovery Grant, Micro Net DND Grant, and the Alliance Quint Grant, and was conducted at the Institute for Quantum Computing, University of Waterloo, which is funded by the Government of Canada through ISED. DT and PS are partially funded by the Mike and Ophelia Lazaridis Fellowship.

A Technical Statements

We use $S_\circ(Q)$ to denote the set of normalized states on Q. We use $S_\bullet(Q)$ to denote the set of all sub-normalized states on Q. We use $\mathrm{Pos}(Q)$ to denote the set of positive semi-definite operators on Q. The smoothing on the min and max entropies is with respect to the purified distance [62, Definition 3.8].

Lemma 6. ([2, Lemma 7]) Let $\rho_{CQ} \in S_\bullet(CQ)$ be classical in C, and let Ω be any event on C such that $\Pr(\Omega)_\rho \leq \varepsilon$. Then there exists a sub-normalized state $\tilde{\rho}_{CQ} \in S_\bullet(CQ)$ with $\Pr(\Omega)_{\tilde{\rho}} = 0$, and $P(\rho, \tilde{\rho}) \leq \sqrt{\varepsilon}$, where P denotes the purified distance.

We use the above lemma in the proof of the following statement. The following statement allows us to replace the smooth max entropy term in the EUR statement with our bound on the phase error rate. The proof is basically the same as the proof of [2, Proposition 8].

Lemma 7. Let $\rho \in S_\bullet(XY)$ where X, Y store n-bit strings, and let $\boldsymbol{e}_{XY}$ denote the error rate in these strings. Let Ω be any event such that $\boldsymbol{e}_{XY} > e_{\max}$, and let $\Pr(\Omega)_\rho \leq \kappa$. For any $e_{\max} < 1/2$, we have

$$H_{\max}^{\sqrt{\kappa}}(X|Y)_\rho \leq nh(e_{\max}) \tag{68}$$

Proof. By Lemma 6, there exists a state $\tilde{\rho}_{XY}$ such that $\Pr(\Omega)_{\tilde{\rho}} = 0$ and $P(\rho, \tilde{\rho}) \leq \sqrt{\kappa}$. Therefore we have

$$\begin{aligned}
H_{\max}^{\sqrt{\kappa}}(X|Y)_\rho &\leq H_{\max}(X|Y)_{\tilde{\rho}} \\
&= \log\left(\sum_{y\in\{0,1\}^n} \Pr(Y=y)_{\tilde{\rho}} 2^{H_{\max}(X|Y)_{\tilde{\rho}|Y=y}}\right) \\
&\leq \max_{y\in\{0,1\}^n} H_{\max}(X|Y)_{\tilde{\rho}|Y=y} \\
&= \max_{y\in\{0,1\}^n} \log\left|\left\{x\in\{0,1\}^n : \Pr(X=x\wedge Y=y)_{\tilde{\rho}} > 0\right\}\right| \\
&\leq \log\left(\sum_{k=0}^{ne_{\max}} \binom{n}{k}\right), \\
&\leq \log\left(2^{nh(e_{\max})}\right)
\end{aligned} \tag{69}$$

where we used the definition of the smooth max entropy in the first inequality, and [63, Sec. 4.3.2] for the second equality. The third inequality and the fourth equality follow from the definitions. The fifth inequality follows from the fact that the state $\tilde{\rho}$ is guaranteed to have $\leq ne_{\max}$ errors, while the final inequality follows from the suitable bound on the sum of binomial coefficients. □

Lemma 1. [Filtering POVMs] Let $\{\Gamma_k | k \in \mathcal{A}\}$ be a POVM on a register Q, and let $\{\mathcal{A}_i\}_{i\in\mathcal{P}_\mathcal{A}}$ be a partition of $\mathcal{A}$, and let $\rho \in S_\bullet(Q)$ be a state. The classical register storing the measurement outcomes when ρ is measured using $\{\Gamma_k\}_{k\in\mathcal{A}}$ is given by

$$\rho_{\text{final}} \coloneqq \sum_{k\in\mathcal{A}} \mathrm{Tr}(\Gamma_k \rho)\, |k\rangle\langle k| \,. \tag{7}$$

This measurement procedure is equivalent (in the sense of being the same quantum to classical channel) to the following two-step measurement procedure: First doing a coarse-grained "filtering" measurement of i, using POVM $\{\tilde{F}_i\}_{i\in\mathcal{P}_\mathcal{A}}$, where

$$\begin{aligned}
\tilde{F}_i &\coloneqq \sum_{j\in\mathcal{A}_i} \Gamma_j, \qquad \text{leading to the post-measurement state} \\
\rho'_{\text{intermediate}} &= \sum_{i\in\mathcal{P}_\mathcal{A}} \sqrt{\tilde{F}_i}\rho\sqrt{\tilde{F}_i}^\dagger \otimes |i\rangle\langle i| \,.
\end{aligned} \tag{8}$$

Upon obtaining outcome i in the first step, measuring using POVM $\{G_k\}_{k\in\mathcal{A}_i}$ where

$$\begin{aligned} G_k &:= \sqrt{\tilde{F}_i}^{+}\Gamma_k\sqrt{\tilde{F}_i}^{+} + P_k \qquad \text{leading to the post-measurement classical state} \\ \rho'_{\text{final}} &= \sum_{i\in\mathcal{P}_\mathcal{A}}\sum_{k\in\mathcal{A}_i}\operatorname{Tr}\left(G_k\sqrt{\tilde{F}_i}\rho\sqrt{\tilde{F}_i}\right)|k\rangle\langle k|\,, \end{aligned} \tag{9}$$

where F^+ denotes the pseudo-inverse of F, and P_k are any positive operators satisfying $\sum_{k\in\mathcal{A}_i}P_k = \mathrm{I} - \Pi_{\tilde{F}_i}$, where $\Pi_{\tilde{F}_i}$ denotes the projector onto the support of $\tilde{F}_i$.

Proof. Observe that $\{\tilde{F}_i|i\in\mathcal{P}_\mathcal{A}\}$ is a valid set of POVMs by construction. Moreover, $\{G_k|k\in\mathcal{A}_i\}$ is a valid set of POVMs for each i, also by construction. Thus we only need to show that $\rho_{\text{final}} = \rho'_{\text{final}}$. Using the cyclicity of trace in Eq. (9), it suffices to prove

$$\sqrt{\tilde{F}_i}G_k\sqrt{\tilde{F}_i} = \Gamma_k \quad \forall i\in\mathcal{P}_\mathcal{A}, \forall k\in\mathcal{A}_i. \tag{70}$$

Substituting the expression for F_k into the above equation, we obtain

$$\begin{aligned} \sqrt{\tilde{F}_i}G_k\sqrt{\tilde{F}_i} &= \sqrt{\tilde{F}_i}\left(\sqrt{\tilde{F}_i}^{+}\Gamma_k\sqrt{\tilde{F}_i}^{+} + P_k\right)\sqrt{\tilde{F}_i} \\ &= \sqrt{\tilde{F}_i}\left(\sqrt{\tilde{F}_i}^{+}\Gamma_k\sqrt{\tilde{F}_i}^{+}\right)\sqrt{\tilde{F}_i} \\ &= \Pi_{\tilde{F}_i}\Gamma_k\Pi_{\tilde{F}_i} \\ &= \Gamma_k, \end{aligned} \tag{71}$$

where the second equality follows from the fact that P_k and $\tilde{F}_i$ have orthogonal supports, and the final equality uses the fact that the support for $\tilde{F}_i$ is larger than the support for Γ_k for $k\in\mathcal{A}_i$. This concludes the proof. □

B Variable-length security proof

In this appendix we will prove the following theorem regarding variable-length security of the protocol from Section 2.

Theorem 1. [Variable-length security of BB84 with qubit source] Suppose Eq. (5) is satisfied and let $\lambda_{\text{EC}}(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ be a function that determines the number of bits used for error-correction. Define

$$\begin{aligned} l(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) := \max\Big(0, n_K\left(1 - h\left(\mathcal{B}_{\delta_1,\delta_2}(e_X^{\text{obs}}, n_X, n_K)\right)\right) - \lambda_{\text{EC}}(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) \\ - 2\log(1/2\varepsilon_{\text{PA}}) - \log(2/\varepsilon_{\text{EV}})\Big), \end{aligned} \tag{6}$$

where $h(x)$ is the binary entropy function for $x\leq 1/2$, and $h(x) = 1$ otherwise. Then the variable-length QKD protocol that produces a key of length $l(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ using $\lambda_{\text{EC}}(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ bits for error-correction, upon the event $\Omega_{(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}\wedge\Omega_{\text{EV}}$ is $(2\varepsilon_{\text{AT}} + \varepsilon_{\text{PA}} + \varepsilon_{\text{EV}})$-secure [8].

Proof. Our proof will consist of three parts. In the first part, we will discuss the security definition for variable-length QKD protocols. In the second part we will use entropic uncertainty relations and Eq. (5) to obtain a suitable lower bound on the smooth min entropy of the raw key register in the QKD protocol. In the third part, we use this to prove variable-length security.

[8] For pedagogical reasons, we ignore the issues arising from non-integer values of hash-lengths. Such issues can be easily fixed by suitable use of floor and ceiling functions.

B.0.1 Variable-length security definition

In order to prove the $\varepsilon_{\text{secure}}$-security of a variable-length QKD protocol [25, 26], one must show that for all attacks by the adversary, the following statement is true :

$$\sum_{l=1}^{\infty} \Pr(\Omega_{\boldsymbol{l}=l}) \frac{1}{2} \left\| \rho_{K_A K_B C^n C_E C_P E^n | \Omega_{\boldsymbol{l}=l}} - \sum_{k \in \{0,1\}^l} \frac{1}{2^l} |kk\rangle\langle kk|_{K_A K_B} \otimes \rho_{C^n C_E C_P E^n | \Omega_{\boldsymbol{l}=l}} \right\|_1 \leq \varepsilon_{\text{secure}} \tag{72}$$

where $\Omega_{\boldsymbol{l}=l}$ denotes the event that a key of length l bits is produced. The error-verification step of the protocol guarantees the ε_{EV}-correctness of the protocol [27]. The fact that $(2\varepsilon_{\text{AT}} + \varepsilon_{\text{PA}})$-secrecy (Eq. (73)) and ε_{EV}-correctness implies $\varepsilon_{\text{secure}} = (2\varepsilon_{\text{AT}} + \varepsilon_{\text{PA}} + \varepsilon_{\text{EV}})$-security of the QKD protocol (Eq. (72)) has already been shown in many prior works [26, 27] and we do not repeat it here. Therefore, in this work we focus on proving the $(2\varepsilon_{\text{AT}} + \varepsilon_{\text{PA}})$-secrecy of the QKD protocol. This requires us to show

$$\sum_{l=1}^{\infty} \Pr(\Omega_{\boldsymbol{l}=l}) \frac{1}{2} \left\| \rho_{K_A C^n C_E C_P E^n | \Omega_{\boldsymbol{l}=l}} - \sum_{k \in \{0,1\}^l} \frac{1}{2^l} |k\rangle\langle k|_{K_A} \otimes \rho_{C^n C_E C_P E^n | \Omega_{\boldsymbol{l}=l}} \right\|_1 \leq 2\varepsilon_{\text{AT}} + \varepsilon_{\text{PA}} \tag{73}$$

which is essentially the same statement as Eq. (72), but with Bob's key register omitted.

B.0.2 Bounding the smooth min entropy

Let us turn our attention to the phase error rate estimate. Let

$$\kappa(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) := \Pr\left(\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}} \geq \mathcal{B}_{\delta_1,\delta_2}(e_X^{\text{obs}}, n_X, n_K) \right)_{|\Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}} \tag{74}$$

where $\kappa(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ denotes the probability that our computed bound $\mathcal{B}_{\delta_1,\delta_2}(e_X^{\text{obs}}, n_X, n_K)$ fails, conditioned on the event $\Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}$. We will not be able to directly bound $\kappa(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ (see footnote. [9]). However note that Eq. (5) trivially implies

$$\begin{aligned} \sum_{n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}} \Pr\left(\Omega_{(n_X, n_K, e_X^{\text{obs}} e_Z^{\text{obs}})}\right) \kappa(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) &= \Pr\left(\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}} \geq \mathcal{B}_{\delta_1,\delta_2}(\boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}}, \boldsymbol{n_X}, \boldsymbol{n_K}) \right) \\ &\leq \varepsilon_{\text{AT}}^2, \end{aligned} \tag{75}$$

where the sum is over all possible values of $n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}$. We will utilize Eq. (75), which follows from Eq. (5), in bounding the smooth min entropy of the raw key register.

To do so, focus on the state $\rho_{A^{n_K} B^{n_K} E^n C^n | \Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}}$, which is the state on the detected key generation rounds. This state can be obtained by transforming Bob's measurement procedure to consist of two steps, and then only implementing the first step measurement which determines the detect vs no-detect outcome. Such a state can be rigorously obtained using Lemma 1 from Section 3. For the purposes of this proof, we only need the fact that it is well defined. We will obtain a bound on the smooth min entropy of the key generated from this state.

Suppose Alice measures her n_K systems in the Z basis. Let the post-measurement state be given by $\rho_{Z_A^{n_K} B^{n_K} E^n C^n | \Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}}$. Suppose she measures it in the X basis, and let the post-measurement state be given by $\rho^{\text{virt}}_{X_A^{n_K} B^{n_K} E^n C^n | \Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}}$. This X measurement is not actually done in the protocol, and is only required for the theoretical proof. Using the entropic uncertainty relation [1], we can relate the smooth min and max entropies $\left(\text{with smoothing parameter } \sqrt{\kappa(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})} \right)$

[9] In fact, it is easy to see that if Eve implements an intercept-resend attack, it is impossible to obtain any non-trivial bounds on $\kappa(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$. This is because during an intercept-resend attack, even if the observations indicate a low error rate (due to an unlucky protocol run), the phase error rate is still equal to 1/2

of the two states obtained via Z and X measurements as

$$\begin{aligned} &H_{\min}^{\sqrt{\kappa(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}}(Z_A^{n_K}|C^nE^n)_{\rho|\Omega_{(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}} \\ &+H_{\max}^{\sqrt{\kappa(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}}(X_A^{n_K}|B^{n_K})_{\rho^{\text{virt}}|\Omega_{(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}} \geq n_K c_q. \end{aligned} \tag{76}$$

where $c_q := \log\left(\frac{1}{\max_{i,j}\left\|\Gamma^{(A)}_{(X,i)}\Gamma^{(A)}_{(Z,j)}\right\|_\infty^2}\right)$. We have deliberately chosen an appropriate smoothing parameter (see Eq. (74) for κ) in the above equation. This choice will play a role at a later stage in the proof.

Remark 17. Notice that the value of c_q *only* depends on the POVM's used by Alice, after using the source-replacement scheme, and is equal to 1 in this work. Thus, we set $c_q = 1$ in the remainder of this work. Moreover, directly using the EUR in this context requires Alice to implement an *active* basis choice measurement, which requires perfect signal state preparation. However, as stated earlier, several techniques of dealing with imperfect source preparation exist.

We can make Bob measure his systems B in the X basis to obtain the classical outcome X_B. Then, using data processing [62, Theorem 6.2], we obtain

$$\begin{aligned} &H_{\min}^{\sqrt{\kappa(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}}(Z_A^{n_K}|C^nE^n)_{\rho|\Omega_{(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}} \\ &+H_{\max}^{\sqrt{\kappa(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}}(X_A^{n_K}|X_B^{n_K})_{\rho^{\text{virt}}|\Omega_{(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}} \geq n_K. \end{aligned} \tag{77}$$

Recall that we have a probabilistic upper bound on $\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}}$ (the error rate in $X_A^{n_K}, X_B^{n_K}$) conditioned on the event $\Omega_{(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}$. This bound fails with probability $\kappa(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})$ (see Eq. (74)). Thus, using Lemma 7 (see Section A) along with this fact, we obtain:

$$H_{\max}^{\sqrt{\kappa(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}}(X_A^{n_K}|X_B^{n_K})_{\rho^{\text{virt}}|\Omega_{(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}} \leq n_K h\left(\mathcal{B}_{\delta_1,\delta_2}(e_X^{\text{obs}},n_X,n_K)\right), \tag{78}$$

which along with Eq. (77) gives us

$$H_{\min}^{\sqrt{\kappa(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}}(Z_A^{n_K}|C^nE^n)_{\rho|\Omega_{(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}} \geq n_K(1-h\left(\mathcal{B}_{\delta_1,\delta_2}(e_X^{\text{obs}},n_X,n_K)\right)). \tag{79}$$

This is the required bound on the smooth min entropy of the raw key. We will now use Eq. (79) to prove the $(2\varepsilon_{\text{AT}}+\varepsilon_{\text{PA}})$-secrecy of the QKD protocol.

B.0.3 Proving variable-length security

To obtain $(2\varepsilon_{\text{AT}}+\varepsilon_{\text{PA}})$-secrecy, we must show that Eq. (73) is true. Note that Eq. (73) groups together terms with the same length of the output key. However, different events $\Omega_{(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}$ may correspond to the same length of the output key. Nevertheless, $\Omega_{(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}$ is a deterministic function of the classical announcements C^n. Thus, the states conditioned on different $\Omega_{(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}$ have orthogonal supports. Therefore, it is enough to show that

$$\begin{aligned} \Delta := \frac{1}{2}\sum_{n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}}} &\Pr\left(\Omega_{(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}\wedge\Omega_{\text{EV}}\right)\left\|\rho_{K_AC^nC_EC_PE^n|\Omega_{(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}\wedge\Omega_{\text{EV}}}\right. \\ -\sum_{k\in\{0,1\}^{l(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}} &\left.\frac{|k\rangle\langle k|_{K_A}}{2^{l(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}}\otimes\rho_{C^nC_EC_PE^n|\Omega_{(n_X,n_K,e_X^{\text{obs}},e_Z^{\text{obs}})}\wedge\Omega_{\text{EV}}}\right\|_1 \leq 2\varepsilon_{\text{AT}}+\varepsilon_{\text{PA}}, \end{aligned} \tag{80}$$

since we can group together terms with the same output key to obtain Eq. (73) from Eq. (80). We will now prove Eq. (80).

Now, note that without loss of generality, we can assume that we are summing over events that lead to a non-trivial length of the key (since events where the protocol aborts do not contribute to

Δ). Let $\mathcal{F} = \{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) | l(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) > 0\}$ be the set of parameters that produce a non-trivial length of the key. Then, Δ can bounded using the following chain of expressions, which we explain below:

$$
\begin{aligned}
\Delta \leq & \sum_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})} \Pr\left(\Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}\right) \left(2\sqrt{\kappa(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})} \right. \\
& \left. + \frac{1}{2} 2^{-\frac{1}{2}\left(H_{\min}^{\sqrt{\kappa(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}} (Z^{n_K} | E^n C^n C_E)_{(\rho | \Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}) \wedge \Omega_{\text{EV}}} - l(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) \right)} \right) \\
\leq & \sum_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})} \Pr\left(\Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}\right) \left(2\sqrt{\kappa(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})} \right. \\
& \left. + \frac{1}{2} 2^{-\frac{1}{2}\left(H_{\min}^{\sqrt{\kappa(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}} (Z^{n_K} | E^n C^n C_E)_{\rho | \Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}} - l(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) \right)} \right) \\
\leq & \sum_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) \in \mathcal{F}} \Pr\left(\Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}\right) \left(2\sqrt{\kappa(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})} \right. \\
& \left. + \frac{1}{2} 2^{-\frac{1}{2}\left(H_{\min}^{\sqrt{\kappa(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}} (Z^{n_K} | E^n C^n)_{\rho | \Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}} - l(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) - \lambda_{\text{EC}}(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) - \log(2/\varepsilon_{\text{EV}}) \right)} \right) \\
\leq & \sum_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) \in \mathcal{F}} \Pr\left(\Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}\right) \left(2\sqrt{\kappa(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})} \right. \\
& \left. + \frac{1}{2} 2^{-\frac{1}{2}\left(n_K \left(1 - h\left(\mathcal{B}_{\delta_1, \delta_2}(e_X^{\text{obs}}, n_X, n_K)\right)\right) - l(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) - \lambda_{\text{EC}}(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) - \log(2/\varepsilon_{\text{EV}}) \right)} \right) \\
= & \sum_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}) \in \mathcal{F}} \Pr\left(\Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}\right) \left(\varepsilon_{\text{PA}} + 2\sqrt{\kappa(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})} \right) \\
\leq & \varepsilon_{\text{PA}} + 2 \sqrt{\sum_{n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}} \Pr\left(\Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}\right) \kappa(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})} \\
\leq & \varepsilon_{\text{PA}} + 2\varepsilon_{\text{AT}}.
\end{aligned}
\tag{81}
$$

Here, we used the leftover-hashing lemma [2, Proposition 9] with the appropriate smoothing parameter on the sub-normalized state $(\rho_{|\Omega_{(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})}})_{\wedge \Omega_{\text{EV}}}$ for the first inequality. Since we use sub-normalized conditioning on Ω_{EV}, it only appears in the smooth min entropy term and not inside the probability. Next, we use [2, Lemma 10] to get rid of the sub-normalized conditioning ($\wedge \Omega_{\text{EV}}$) in the smooth min entropy term in the second inequality. We used [62, Lemma 6.8] to split off the error-correction information ($\lambda_{\text{EC}}(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$) and error-verification information ($\log(2/\varepsilon_{\text{EV}})$) in the third inequality. We used the bound on the smooth min entropy from Eq. (79) for the fourth inequality, and the values of $l(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ and $\lambda_{\text{EC}}(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ from Eq. (6) for the fifth equality. We used concavity of the square root function and Jensen's inequality to pull the sum over probabilities inside the square root for the sixth inequality, and Eq. (75) for the final inequality.

□

Remark 18. Note that the critical step here was using the concavity of the square root function to see that a bound on the *average* failure probability of the phase error estimation procedure is enough to prove security. This is the same fundamental trick used by Ref. [9, 30, 31]. Our presentation here is in the EUR framework, where this manifests in the deliberate choice of our smoothing parameter in the first part of the proof.

Remark 19. Notice that in the variable-length protocol for which we proved security, the number of bits on which privacy amplification is applied is variable. It depends on the number of key

generation rounds obtained in each protocol run. Some subtle issues regarding two-universal hashing on a variable-length *input* register were pointed out and addressed in [27, Section VII]. In particular, it was noted that first looking at the number of bits in the raw key, and then choosing an appropriate two-universal hashing procedure for that many input bits, *does not produce a valid two-universal hashing procedure on the input space of variable-length bit strings*. Due to this, the leftover-hashing lemma cannot be straightforwardly applied to such a scenario. However, this issue was addressed by showing that when the locations of the discard rounds are publicly announced, the theoretical analyses of scenarios where the rounds are actually discarded, vs mapped to special symbols such as 0 or $\perp$ (where leftover-hashing lemma can be applied), are equivalent [27, Lemmas 4, 5]. Due to this equivalence, the PA procedure described above can be applied in QKD protocols.

It is interesting to note that these issues are completely avoided by the above proof, in a very *different* manner than [27]. This is because in this proof, we always apply the leftover-hashing lemma on a state conditioned on the specific length of the raw key register (Eq. (79)). Therefore, the leftover-hashing lemma can be applied in a straightforward manner, and there are no issues is choosing the hashing family based on the specific length of the raw key register. In other words, the PA procedure described above is valid for this proof. In a similar sense, the variable-length security proof from [27] critically relied on a technical lemma (Lemma 9), that necessitated the use of Rényi entropies instead of smooth min entropy in that work. However, the variable-length proof presented above takes a different approach, and does *not* impose the same requirements on the behavior of smooth min entropy. Again, this is due to the use of Eq. (79).

B.1 Comparing to fixed-length protocols

We will now compare the results obtain above with the key rate obtained for fixed-length protocols. Consider a fixed-length protocol that is identical to the steps in Section 2, except that it accepts if and only if $n_X \geq n_X^L$, $n_K \geq n_K^L$, $e_X^{\text{obs}} \leq e_X^U$, and $e_Z^{\text{obs}} \leq e_Z^U$. Then, the key length obtained for such a protocol can be shown to be the same expressions as Eq. (6), with $n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}}$ replaced with the acceptance thresholds $n_K^L, n_K^L, e_X^U, e_Z^U$. Since $l(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ is an increasing function in n_X, n_K and a decreasing function of $e_X^{\text{obs}}, e_Z^{\text{obs}}$, the variable-length protocol *always produces at least as much key as* the the fixed-length protocol, for any possible observations $(n_X, n_K, e_X^{\text{obs}}, e_Z^{\text{obs}})$ during a protocol run (for the above proof technique).

Furthermore,theoretical works with such acceptance conditions typically require Alice and Bob to pick a uniformly random sample of n_X^L rounds for testing, and n_K^L rounds for key generation (in the highly-likely event that they obtain extra rounds) [3, 35, 47]. This requires additional randomness in the protocol implementation. The variable-length version does not require this step, and therefore had a reduced requirement on local randomness.

C Sampling

In this section, we prove the technical statements needed to prove our sampling bounds.

C.1 Random Sampling

We start with the usual Serfling [41] statement in the following lemma. The following lemma is obtained from [2, Eq. 74, Lemma 6]

Lemma 8 (Serfling)**.** Let $\boldsymbol{X}_1 \dots \boldsymbol{X}_{m+n}$ be bit-valued random variables. Let $\boldsymbol{J}_m$ denote the choice of a uniformly random subset of m positions, out of $m+n$ positions. Then,

$$\begin{aligned} \Pr\left(\sum_{i \notin \boldsymbol{J}_m} \frac{\boldsymbol{X}_i}{n} \geq \sum_{i \in \boldsymbol{J}_m} \frac{\boldsymbol{X}_i}{m} + \gamma_{\text{serf}} \right) &\leq e^{-2\gamma_{\text{serf}}^2 f_{\text{serf}}(m,n)}, \\ f_{\text{serf}}(m,n) &:= \frac{nm^2}{(n+m)(m+1)}. \end{aligned} \tag{82}$$

Serfling basically states that if one chooses a random set of positions, then the fraction of 1s in those positions gives us a good estimate of the fraction of 1s in the remaining positions.

However, observe that the sampling procedure in the protocol from Sections 3.3 and 4.4 does not actually choose a random subset of fixed-length for testing. Instead, the protocol decides to map each conclusive round to test or key in an IID manner. Therefore, the application of the Serfling bound is not straightforward. In the following lemma, we show how the Serfling bound can still be rigorously used.

Lemma 2. [Serfling with IID sampling] Let $\boldsymbol{X}_1 \dots \boldsymbol{X}_n$ be bit-valued random variables. Suppose each position i is mapped to the "test set" ($i \in \boldsymbol{J}_t$) with probability p_t, and the "key set" ($i \in \boldsymbol{J}_k$) with probability p_k. Let $\Omega_{(n_X,n_K)}$ be the event that exactly n_X positions are mapped to test, and exactly n_K positions are mapped to key. Then, conditioned on the event $\Omega_{(n_X,n_K)}$, the following statement is true:

$$\begin{aligned} \Pr\left(\sum_{i\in\boldsymbol{J}_k}\frac{\boldsymbol{X}_i}{n_K} \geq \sum_{i\in\boldsymbol{J}_t}\frac{\boldsymbol{X}_i}{n_X} + \gamma_{\text{serf}}\right)_{|\Omega_{(n_X,n_K)}} &\leq e^{-2\gamma_{\text{serf}}^2 f_{\text{serf}}(n_X,n_K)}, \\ f_{\text{serf}}(n_X,n_K) &\coloneqq \frac{n_K n_X^2}{(n_K+n_X)(n_X+1)}. \end{aligned} \tag{11}$$

Proof. Since the sampling procedure randomly assigns each bit to test or key (or does nothing with them if $p_t + p_k < 1$), Lemma 8 cannot be directly applied. However, consider what happens if we condition on the event $\Omega_{(n_X,n_K)}$. Then, for a given set of positions that form the $n_X + n_K$ positions selected for test or key, it is the case that each set of n_X positions is equally likely. Therefore, the above sampling procedure is exactly equivalent to:

1. First determining the event $\Omega_{(n_X,n_K)}$ by sampling from *some* probability distribution.
2. Pick some $n_X + n_K$ positions at random.
3. Then determining the exact positions of the n_X test rounds, by choosing a random subset of fixed-size n_X out of these $n_X + n_K$ positions.

The necessary claim follows by applying Lemma 8 for step 3 of the above procedure. □

C.2 Sampling with imperfect detectors

We now turn our attention to proving Lemma 3, which is the main statement utilized in extending the EUR approach to imperfect detectors in Section 4. We start by proving Lemmas 4 and 9 which we use later in the proof of Lemma 10.

Recall our notation: If $\rho_{Q^n} \in S_\circ(Q^{\otimes n})$ is an arbitrary state, and $\{P_1, P_2, \dots, P_m\}$ is a set of POVM elements, then we let $\boldsymbol{N}_{P_i}$ denote the classical random variable corresponding to the number of measurement outcomes corresponding to P_i when the state ρ_{Q^n} is measured. Moreover, let $\boldsymbol{D}_P$ denote the classical random variable that describes the measurement outcomes when each subsystem of ρ is measured using $\{P_1, P_2, \dots, P_m\}$. We use $S \sim \boldsymbol{D}_P$ to denote the statement S is sampled from $\boldsymbol{D}_P$.

Lemma 9. Let $\rho_{Q^n} \in S_\circ(Q^{\otimes n})$ be an arbitrary state. Let $\{P, I-P\}$ and $\{P', I-P'\}$ be two sets of POVM elements such that $P \leq P'$. Then, for any e, it is the case that

$$\Pr\left(\frac{\boldsymbol{N}_P}{n} \geq e\right) \leq \Pr\left(\frac{\boldsymbol{N}_{P'}}{n} \geq e\right) \tag{83}$$

Proof. We will describe a procedure to generate random strings S, S' such that $S \sim \boldsymbol{D}_P, S' \sim \boldsymbol{D}'_P$. Consider the POVM $\{P, P'-P, I-P'\}$, and let T be the classical string taking values in $\{0,1,2\}^n$ which stores the measurement outcomes when measured using this POVM. Then, S, S' can be obtained by first obtaining T, followed by the following remapping

$$(S_i, S'_i) = \begin{cases} (1,1) & T_i = 0 \\ (0,1) & T_i = 1 \\ (0,0) & T_i = 2 \end{cases}$$

where i denotes the position in the string. The required claim follows from the observation that the above procedure maps more S'_i to 1 than S_i. Thus,

$$\Pr(w(\boldsymbol{S}') \geq w(\boldsymbol{S})) \geq 0 \implies \Pr(w(\boldsymbol{S}') > ne) \geq \Pr(w(\boldsymbol{S}) \geq ne) \tag{84}$$

where w denotes the hamming weight of the string (sum of each element of the string). The necessary statement follows after noting that $w(S) \sim \boldsymbol{N}_P$ and $w(S') \sim \boldsymbol{N}_{P'}$ (which can be argued rigorously using the two-step measurement Lemma 1). □

Remark 20. Note a conceptual subtlety in the above proof: The procedure used to generate S, S' in the above proof has some joint probability distribution associated to it. This means that (S, S') is a well-defined random variable. However, one cannot talk about the joint probability distribution of two different sets of measurement on the same quantum state. This subtle issue is avoided by noting that we are only interested in making statements on the marginal probability distribution of S and S', and how they relate to one another. And it is indeed true that these distributions satisfy $S \sim \boldsymbol{D}_P$ and $S' \sim \boldsymbol{D}_{P'}$, which is enough to prove our claim. The fact that S, S' has some joint distribution associated with it is immaterial.

Lemma 4. [Small POVM measurement] Let $\rho_{Q^n} \in S_\circ(Q^{\otimes n})$ be an arbitrary state. Let $\{P, I - P\}$ be a POVM such that $\|P\|_\infty \leq \delta$. Then

$$\Pr\left(\frac{\boldsymbol{N}_P}{n} \geq \delta + c\right) \leq F(n, \delta, c) \coloneqq \sum_{i=n(\delta+c)}^{n} \binom{n}{i} \delta^i (1-\delta)^{n-i}, \tag{29}$$

where $\boldsymbol{N}_P$ is the number of P-outcomes when each subsystem of ρ_{Q^n} is measured using POVM $\{P, \mathrm{I} - P\}$.

Proof. Since $\|P\|_\infty \leq \delta$, we have $P \leq \delta I$. By Lemma 9, we have

$$\Pr\left(\frac{\boldsymbol{N}_P}{n} \geq \delta + c\right) \leq \Pr\left(\frac{\boldsymbol{N}_{\delta I}}{n} \geq \delta + c\right) \tag{85}$$

Observe that measurement using $\{\delta I, (1-\delta)I\}$ is equivalent to Bernoulli sampling. Thus $\boldsymbol{N}_{\delta I}$ obeys the binomial distribution. Therefore,

$$\Pr\left(\frac{\boldsymbol{N}_{\delta I}}{n} \geq \delta + c\right) \leq \sum_{i=n(\delta+c)}^{n} \binom{n}{i} \delta^i (1-\delta)^{n-i}. \tag{86}$$

□

Lemma 10. Let $\rho_{Q^n} \in S_\circ(Q^{\otimes n})$ be an arbitrary state. Let $\{P, I - P\}$ and $\{P', I - P'\}$ be two sets of POVM elements. Suppose there exists a $0 \leq \tilde{P} \leq I$ such that $P \leq \tilde{P}, P' \leq \tilde{P}$, and $\left\|\tilde{P} - P\right\|_\infty \leq \delta$. Then

$$\Pr\left(\frac{\boldsymbol{N}_{P'}}{n} \geq e + (\delta + c)\right) \leq \Pr\left(\frac{\boldsymbol{N}_P}{n} \geq e\right) + F(n, \delta, c), \tag{87}$$

where $F(n, \delta, c)$ was defined in Lemma 4.

Proof. We will describe a process to generate $S \sim \boldsymbol{D}_P$ and $\tilde{S} \sim \boldsymbol{D}_{\tilde{P}}$, in a similar manner as in the proof of Lemma 9. In particular, let T be the random variable taking values in $\{0, 1, 2\}^n$ that stores the measurement outcomes of $\{P, \tilde{P} - P, I - \tilde{P}\}$ measurements. We generate $S, \tilde{S}$ by first obtaining T, followed by the following remapping

$$(S_i, \tilde{S}_i) = \begin{cases} (1,1) & T_i = 0 \\ (0,1) & T_i = 1 \\ (0,0) & T_i = 2. \end{cases}$$

Then,

$$\begin{aligned}
\Pr(\boldsymbol{N}_{\tilde{P}} \geq ne + n(\delta + c)) &= \Pr\Big(w(\tilde{\boldsymbol{S}}) \geq ne + n(\delta + c)\Big) \\
&= \Pr\Big(w(\tilde{\boldsymbol{S}}) \geq ne + n(\delta + c) \cap w(\boldsymbol{S}) \geq ne\Big) \\
&+ \Pr\Big(w(\tilde{\boldsymbol{S}}) \geq ne + n(\delta + c) \cap w(\boldsymbol{S}) < ne\Big) \\
&\leq \Pr(w(\boldsymbol{S}) \geq ne) + \Pr\Big(w(\tilde{\boldsymbol{S}}) - w(\boldsymbol{S}) \geq n(\delta + c)\Big) \\
&= \Pr(\boldsymbol{N}_P \geq ne) + \Pr\big(\boldsymbol{N}_{\tilde{P}-P} \geq n(\delta + c)\big) \\
&\leq \Pr(\boldsymbol{N}_P \geq ne) + F(n, \delta, c).
\end{aligned} \tag{88}$$

where we used Lemma 4 in the final inequality, the fact that $w(S) \sim \boldsymbol{N}_P$ and $w(\tilde{S}) - w(S) = w(\tilde{S} - S) \sim \boldsymbol{N}_{\tilde{P}-P}$ ($\tilde{S}_i - S_i = 1$ if and only if $T_i = 1$) for the penultimate inequality, and basic properties of probabilities for the remaining steps. Next, we replace the $\tilde{P}$ with P' using Lemma 9 and $\tilde{P} \geq P'$, and obtain

$$\Pr(\boldsymbol{N}_{P'} \geq ne + n(\delta + c)) \leq \Pr(\boldsymbol{N}_{\tilde{P}} \geq ne + n(\delta + c)). \tag{89}$$

The proof follows after noting that Eqs. (88) and (89) $\implies$ Eq. (87). □

Lemma 10 above requires an explicit construction of a $\tilde{P}$ satisfying the necessary requirements. However, this requirement can be removed, and we obtain a sightly worse result with greater generality below.

Lemma 3. [Similar measurements lead to similar observed frequencies] Let $\rho_{Q^n} \in S_\circ(Q^{\otimes n})$ be an arbitrary state. Let $\{P, \mathrm{I} - P\}$ and $\{P', \mathrm{I} - P'\}$ be two sets of POVM elements, such that $\|P' - P\|_\infty \leq \delta$. Then,

$$\Pr\left(\frac{\boldsymbol{N}_{P'}}{n} \geq e + 2\delta + c\right) \leq \Pr\left(\frac{\boldsymbol{N}_P}{n} \geq e\right) + F(n, 2\delta, c), \tag{24}$$

for $e \in [0, 1]$, where $\boldsymbol{N}_P$ is the number of P-outcomes when each subsystem of ρ_{Q^n} is measured using POVM $\{P, \mathrm{I} - P\}$, and

$$F(n, \delta, c) \coloneqq \sum_{i=n(\delta+c)}^{n} \binom{n}{i} \delta^i (1 - \delta)^{n-i}. \tag{25}$$

Proof. Let $G' = (1 - \delta)P'$, and $G = (1 - \delta)P$. Using $0 \leq G \leq P$ and Lemma 9, we obtain

$$\Pr(\boldsymbol{N}_G \geq ne) \leq \Pr(\boldsymbol{N}_P \geq ne). \tag{90}$$

Using $0 \leq G' + \delta I \leq I$, $G' + \delta I \geq G$, $\|G' + \delta I - G\|_\infty \leq \delta + \delta(1 - \delta) \leq 2\delta$, and Eq. (88), we obtain

$$\Pr(\boldsymbol{N}_{G'+\delta I} \geq ne + n(2\delta + c)) \leq \Pr(\boldsymbol{N}_G \geq ne) + F(n, 2\delta, c), \tag{91}$$

Finally, using $G' + \delta I \geq P'$, and Lemma 9, we obtain

$$\Pr(\boldsymbol{N}_{P'} \geq ne + n(2\delta + c)) \leq \Pr(\boldsymbol{N}_{G'+\delta I} \geq ne + n(2\delta + c)). \tag{92}$$

The proof follows from the observation that Eqs. (90) to (92) $\implies$ Eq. (24). □

C.3 Sampling with independent imperfect detectors

The statements above are written for a measurement procedure where the same POVM is used to measure each round of the state. However the proofs do not actually use this fact. The same proofs are valid even if the measurement for each round is done using a different POVM element (as long it satisfies the required bounds on the ∞-norm). Thus we write a generalized version of Lemmas 3 and 10 below. They can be proved by simply redoing the proofs in the earlier section.

Lemma 11. Let $\rho_{Q^n} \in S_\circ(Q^{\otimes n})$ be an arbitrary state. Suppose the ith round is measured using POVM $\{P(i), I - P(i)\}$ and let $\boldsymbol{N}_P$ be the number of outcomees corresponding to the first POVM element. Similarly, suppose the ith round is measured using POVM $\{P'(i), \mathrm{I} - P'(i)\}$ and let $\boldsymbol{N}_{P'}$ be the number of outcomes corresponding to the first POVM element. Suppose for all i, there exists a $0 \leq \tilde{P}(i) \leq I$ such that $P(i) \leq \tilde{P}(i), P'(i) \leq \tilde{P}(i)$, and $\left\|\tilde{P}(i) - P(i)\right\|_\infty \leq \delta$. Then

$$\Pr\left(\frac{\boldsymbol{N}_{P'}}{n} \geq e + (\delta + c)\right) \leq \Pr\left(\frac{\boldsymbol{N}_P}{n} \geq e\right) + F(n, \delta, c), \tag{93}$$

where $F(n, \delta, c)$ was defined in Lemma 4.

Lemma 12. Let $\rho_{Q^n} \in S_\circ(Q^{\otimes n})$ be an arbitrary state. Suppose the ith round is measured using POVM $\{P(i), I - P(i)\}$ and let $\boldsymbol{N}_P$ be the number of outcomees corresponding to the first POVM element. Similarly, suppose the ith round is measured using POVM $\{P'(i), \mathrm{I} - P'(i)\}$ and let $\boldsymbol{N}_{P'}$ be the number of outcomes corresponding to the first POVM element. Suppose $\|P'(i) - P(i)\|_\infty \leq \delta \quad \forall i$. Then

$$\Pr\left(\frac{\boldsymbol{N}_{P'}}{n} \geq e + 2\delta + c\right) \leq \Pr\left(\frac{\boldsymbol{N}_P}{n} \geq e\right) + F(n, 2\delta, c), \tag{94}$$

where $F(n, \delta, c)$ was defined in Lemma 4.

D Combining bounds

In this section, we will combine Eqs. (20), (23), (28) and (31) and obtain Eq. (32). This process is simply some cumbersome algebra and the use of the union bound for probabilities.

Combining Eqs. (20) and (23), we obtain

$$\begin{aligned}
&\Pr\left(\tilde{\boldsymbol{e}}^{\mathrm{key}}_{\boldsymbol{XX}} \geq \boldsymbol{e}^{\mathrm{obs}}_{\boldsymbol{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\mathrm{serf}}(\tilde{n}_X, \tilde{n}_K)\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} \\
&= \Pr\left(\left(\tilde{\boldsymbol{e}}^{\mathrm{key}}_{\boldsymbol{XX}} \geq \boldsymbol{e}^{\mathrm{obs}}_{\boldsymbol{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\mathrm{serf}}(\tilde{n}_X, \tilde{n}_K)\right) \bigcap \left(\tilde{\boldsymbol{e}}^{\mathrm{obs}}_{\boldsymbol{XX}} \geq \boldsymbol{e}^{\mathrm{obs}}_{\boldsymbol{X}}\right)\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} \\
&+ \Pr\left(\left(\tilde{\boldsymbol{e}}^{\mathrm{key}}_{\boldsymbol{XX}} \geq \boldsymbol{e}^{\mathrm{obs}}_{\boldsymbol{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\mathrm{serf}}(\tilde{n}_X, \tilde{n}_K)\right) \bigcap \left(\tilde{\boldsymbol{e}}^{\mathrm{obs}}_{\boldsymbol{XX}} < \boldsymbol{e}^{\mathrm{obs}}_{\boldsymbol{X}}\right)\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} \\
&\leq \Pr\left(\tilde{\boldsymbol{e}}^{\mathrm{obs}}_{\boldsymbol{XX}} \geq \boldsymbol{e}^{\mathrm{obs}}_{\boldsymbol{X}}\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} + \Pr\left(\tilde{\boldsymbol{e}}^{\mathrm{key}}_{\boldsymbol{XX}} \geq \tilde{\boldsymbol{e}}^{\mathrm{obs}}_{\boldsymbol{XX}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\mathrm{serf}}(\tilde{n}_X, \tilde{n}_K)\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} \\
&\leq \varepsilon^2_{\text{AT-a}}.
\end{aligned} \tag{95}$$

We will now combine Eqs. (28) and (95). To do so we will additionally need to condition on e^{obs}_X. However, note that Eq. (28) remains true with this additional conditioning (because e^{obs}_X is observed on a different set of rounds). Thus we obtain

$$\begin{aligned}
&\Pr\left(\tilde{\boldsymbol{e}}^{\mathrm{key}}_{\boldsymbol{ZX}} \geq \boldsymbol{e}^{\mathrm{obs}}_{\boldsymbol{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\mathrm{serf}}(\tilde{n}_X, \tilde{n}_K) + \delta_1 + \gamma^{\varepsilon_{\text{AT-b}}}_{\mathrm{bin}}(\tilde{n}_K, \delta_1)\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} \\
&= \sum_{e^{\mathrm{obs}}_X} \Pr\left(\Omega_{(e^{\mathrm{obs}}_X)} | \Omega_{(\tilde{n}_X, \tilde{n}_K)}\right) \Pr\left(\tilde{\boldsymbol{e}}^{\mathrm{key}}_{\boldsymbol{ZX}} \geq e^{\mathrm{obs}}_X + \gamma^{\varepsilon_{\text{AT-a}}}_{\mathrm{serf}}(\tilde{n}_X, \tilde{n}_K) + \delta_1 + \gamma^{\varepsilon_{\text{AT-b}}}_{\mathrm{bin}}(\tilde{n}_K, \delta_1)\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K, e^{\mathrm{obs}}_X)}} \\
&\leq \sum_{e^{\mathrm{obs}}_X} \Pr\left(\Omega_{(e^{\mathrm{obs}}_X)} | \Omega_{(\tilde{n}_X, \tilde{n}_K)}\right) \Pr\left(\tilde{\boldsymbol{e}}^{\mathrm{key}}_{\boldsymbol{XX}} \geq e^{\mathrm{obs}}_X + \gamma^{\varepsilon_{\text{AT-a}}}_{\mathrm{serf}}(\tilde{n}_X, \tilde{n}_K)\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K, e^{\mathrm{obs}}_X)}} + \frac{\varepsilon^2_{\text{AT-b}}}{2} \\
&= \Pr\left(\tilde{\boldsymbol{e}}^{\mathrm{key}}_{\boldsymbol{XX}} \geq \boldsymbol{e}^{\mathrm{obs}}_{\boldsymbol{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\mathrm{serf}}(\tilde{n}_X, \tilde{n}_K)\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} + \frac{\varepsilon^2_{\text{AT-b}}}{2} \\
&\leq \varepsilon^2_{\text{AT-a}} + \varepsilon^2_{\text{AT-b}}.
\end{aligned} \tag{96}$$

where the first equality follows from the definition of conditional probability. The second inequality is obtained by setting $e = e^{\mathrm{obs}}_X + \gamma^{\varepsilon_{\text{AT-a}}}_{\mathrm{serf}}(\tilde{n}_X, \tilde{n}_K)$ in Eq. (28), the third equality follows from the definition of probability and the final inequality follows from Eq. (95)

Combing Eqs. (31) and (96), we obtain

$$
\begin{aligned}
&\Pr\left(\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}} \geq \frac{\boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}} + \gamma_{\text{serf}}^{\varepsilon_{\text{AT-a}}}(\tilde{n}_X, \tilde{n}_K) + \delta_1 + \gamma_{\text{bin}}^{\varepsilon_{\text{AT-b}}}(\tilde{n}_K, \delta_1)}{(1 - \delta_2 - \gamma_{\text{bin}}^{\varepsilon_{\text{AT-c}}}(\tilde{n}_K, \delta_2))}\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} \\
&= \Pr\left(\left(\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}} \geq \frac{\boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}} + \gamma_{\text{serf}}^{\varepsilon_{\text{AT-a}}}(\tilde{n}_X, \tilde{n}_K) + \delta_1 + \gamma_{\text{bin}}^{\varepsilon_{\text{AT-b}}}(\tilde{n}_K, \delta_1)}{(1 - \delta_2 - \gamma_{\text{bin}}^{\varepsilon_{\text{AT-c}}}(\tilde{n}_K, \delta_2))}\right) \bigcap \left(\tilde{\boldsymbol{e}}_{\boldsymbol{ZX}}^{\text{key}} \leq \boldsymbol{e}_{\boldsymbol{X}}^{\text{key}}(1 - \delta_2 - \gamma_{\text{bin}}^{\varepsilon_{\text{AT-c}}}(\tilde{n}_K, \delta_2))\right)\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} \\
&+ \Pr\left(\left(\boldsymbol{e}_{\boldsymbol{X}}^{\text{key}} \geq \frac{\boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}} + \gamma_{\text{serf}}^{\varepsilon_{\text{AT-a}}}(\tilde{n}_X, \tilde{n}_K) + \delta_1 + \gamma_{\text{bin}}^{\varepsilon_{\text{AT-b}}}(\tilde{n}_K, \delta_1)}{(1 - \delta_2 - \gamma_{\text{bin}}^{\varepsilon_{\text{AT-c}}}(\tilde{n}_K, \delta_2))}\right) \bigcap \left(\tilde{\boldsymbol{e}}_{\boldsymbol{ZX}}^{\text{key}} > \boldsymbol{e}_{\boldsymbol{X}}^{\text{key}}(1 - \delta_2 - \gamma_{\text{bin}}^{\varepsilon_{\text{AT-c}}}(\tilde{n}_K, \delta_2))\right)\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} \\
&\leq \Pr\left(\tilde{\boldsymbol{e}}_{\boldsymbol{ZX}}^{\text{key}} \leq \boldsymbol{e}_{\boldsymbol{X}}^{\text{key}}(1 - \delta_2 - \gamma_{\text{bin}}^{\varepsilon_{\text{AT-c}}}(\tilde{n}_K, \delta_2))\right)_{|\Omega_{(\tilde{n}_X, \tilde{n}_K)}} \\
&+ \Pr\left(\tilde{\boldsymbol{e}}_{\boldsymbol{ZX}}^{\text{key}} \geq \boldsymbol{e}_{\boldsymbol{X}}^{\text{obs}} + \gamma_{\text{serf}}^{\varepsilon_{\text{AT-a}}}(\tilde{n}_X, \tilde{n}_K) + \delta_1 + \gamma_{\text{bin}}^{\varepsilon_{\text{AT-b}}}(\tilde{n}_K, \delta_1)\right) \leq \varepsilon_{\text{AT-a}}^2 + \varepsilon_{\text{AT-b}}^2 + \varepsilon_{\text{AT-c}}^2,
\end{aligned}
\tag{97}
$$

which is the required result.

E Decoy Analysis

In this section, we will rigorously justify the application of Hoeffdings concentration inequality [64] in the decoy analysis of this work. To do so, we will first state the following general lemma.

Lemma 13. Let $\boldsymbol{X}_1 \dots \boldsymbol{X}_n$ be random variables. Let X_i be a specific value taken by the random variable $\boldsymbol{X}_i$. For each i, a new random variable $\boldsymbol{Y}_i$ is generated from X_i via the probability distribution $\Pr(\boldsymbol{Y}_i|X_i)$. Then

$$
\Pr\left(\left|\sum_i (\boldsymbol{Y}_i)_{|\Omega(X_1 \dots X_{n_O})} - \mathrm{E}\left(\sum_i (\boldsymbol{Y}_i)_{|\Omega(X_1 \dots X_{n_O})}\right)\right| \geq t\right) \leq 2\exp\left\{\frac{-2t^2}{\sum_i (b_i - a_i)^2}\right\} \tag{98}
$$

where $[a_i, b_i]$ denotes the range of $\boldsymbol{Y}_i$, and E denotes the expectation value. (Note that we do not require the $\boldsymbol{X}_i$s to be independent random variables, nor do we require the $\boldsymbol{Y}_i$s to be independent random variables).

Proof. Fix a specific sequence $X_1 \dots X_n$ of values taken by the random variables $\boldsymbol{X}_i$s. The variables $\boldsymbol{Y}_i$, conditioned on this specific input $X_1 \dots X_n$, are then *independent* random variables (since they are generated by $\Pr(\boldsymbol{Y}_i|X_i)$). Thus, Hoeffding's inequality applies. □

The above lemma is utilized to perform decoy analysis in the following lemma.

Lemma 14. In the decoy-state QKD protocol of Section 5, fix an outcome O, and intensity μ_k. Then, we have

$$
\Pr\left(\left|\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_k}} - \sum_{m=0}^{\infty} p_{\mu_k|m} \boldsymbol{n}_{\boldsymbol{O},\boldsymbol{m}}\right| \geq \sqrt{\frac{\boldsymbol{n}_{\boldsymbol{O}}}{2} \ln\left(\frac{2}{\varepsilon_{\text{AT-d}}^2}\right)}\right) \leq \varepsilon_{\text{AT-d}}^2. \tag{99}
$$

Proof. Consider all the rounds where O is observed. Condition on the event that n_O such rounds are observed. Let $X_1 \dots X_{n_O}$ be the sequence of photon numbers of Alice's signals corresponding to these rounds. Condition further on the event that a specific sequence $X_1 \dots X_{n_O}$ is observed.

Fix an intensity μ_k of interest. Define $\boldsymbol{Y}_i$ as

$$
\boldsymbol{Y}_i \coloneqq \begin{cases} 1 & \text{if intensity } \mu_k \text{ is assigned to the } i\text{th round} \\ 0 & \text{if intensity } \mu_k \text{ is not assigned to the } i\text{th round.} \end{cases} \tag{100}
$$

Since the intensity of each round is chosen from a probability distribution that only depends on the photon number of each round, each $\boldsymbol{Y}_i$ is generated independently via $\Pr(\boldsymbol{Y}_i|X_i)$. By the

construction of $\boldsymbol{Y}_i$s, $\sum_i \boldsymbol{Y}_i = \boldsymbol{n_{O,\mu_k}}$. By the construction of X_is, $|\{i|X_i = m\}| = n_{O,m}$. Then $\mathrm{E}\left(\sum_i(\boldsymbol{Y}_i|X_i)\right) = \sum_{m=0}^{\infty} p_{\mu_k|m} n_{O,m}$. Applying Lemma 13, we directly obtain

$$\Pr\left(\left|\boldsymbol{n_{O,\mu_k}} - \sum_{m=0}^{\infty} p_{\mu_k|m} n_{O,m}\right| \geq t\right)_{|\Omega(X_1 \ldots X_{n_O}, n_O)} \leq 2\exp\left\{\frac{-2t^2}{n_O}\right\}. \tag{101}$$

The above statement is valid for all $X_1 \ldots X_{n_O}$ compatible with $n_O, n_{O,\vec{m}}$. We now obtain a statement that only conditions on n_O via

$$\begin{aligned}
&\Pr\left(\left|\boldsymbol{n_{O,\mu_k}} - \sum_{m=0}^{\infty} p_{\mu_k|m} \boldsymbol{n_{O,m}}\right| \geq t\right)_{|\Omega(n_O)} \\
&= \sum_{X_1 \ldots X_{n_O}} \Pr\left(\Omega_{(X_1 \ldots X_{n_O})}|\Omega_{(n_O)}\right) \Pr\left(\left|\boldsymbol{n_{O,\mu_k}} - \sum_{m=0}^{\infty} p_{\mu_k|m} n_{O,m}\right| \geq t\right)_{|\Omega(X_1 \ldots X_{n_O}, n_O)} \\
&\leq \sum_{X_1 \ldots X_{n_O}} \Pr\left(\Omega_{(X_1 \ldots X_{n_O})}|\Omega_{(n_O)}\right) 2\exp\left\{\frac{-2t^2}{n_O}\right\} \\
&= 2\exp\left\{\frac{-2t^2}{n_O}\right\}.
\end{aligned} \tag{102}$$

Setting $t = \sqrt{\frac{n_O}{2}\ln\left(\frac{2}{\varepsilon^2_{\text{AT-d}}}\right)}$, we obtain

$$\Pr\left(\left|\boldsymbol{n_{O,\mu_k}} - \sum_{m=0}^{\infty} p_{\mu_k|m} \boldsymbol{n_{O,m}}\right| \geq \sqrt{\frac{n_O}{2}\ln\left(\frac{2}{\varepsilon^2_{\text{AT-d}}}\right)}\right)_{|\Omega_{(n_O)}} \leq \varepsilon^2_{\text{AT-d}}, \tag{103}$$

which directly implies the required statement.

□

F Variable-length security proof for decoy-state BB84

In this appendix, we will prove the following theorem regarding the variable-length security of the decoy-state BB84 protocol.

Theorem 3. [Variable-length security of decoy-state BB84] Suppose Eq. (38) is satisfied and let $\lambda_{\text{EC}}(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_Z)$ be a function that determines the number of bits used for error-correction in the QKD protocol. Define

$$\begin{aligned}
l(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_Z) := \max\Bigg(0, \mathcal{B}_1\left(n_{K,\mu_{\vec{k}}}\right)\left(1 - h\left(\mathcal{B}_e\left(e^{\text{obs}}_{X,\mu_{\vec{k}}}, n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}\right)\right)\right) \\
- \lambda_{\text{EC}}(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_Z) - 2\log(1/2\varepsilon_{\text{PA}}) - \log(2/\varepsilon_{\text{EV}})\Bigg)
\end{aligned} \tag{53}$$

where $h(x)$ is the binary entropy function for $x \leq 1/2$, and $h(x) = 1$ otherwise. Then the variable-length decoy-state QKD protocol that produces a key of length $l(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_Z)$ using $\lambda_{\text{EC}}(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_Z)$ bits for error-correction, upon the event $\Omega_{(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\text{obs}}_{X,\mu_{\vec{k}}}, e^{\text{obs}}_Z)} \wedge \Omega_{\text{EV}}$ is $(2\varepsilon_{\text{AT}} + \varepsilon_{\text{PA}} + \varepsilon_{\text{EV}})$-secure.

Proof. Again, the proof is similar to that of Theorem 1 with some differences. The first part of the proof is identical to that of Theorem 1 and we do not repeat it here. Thus, this proof consists of two parts. In the first part, we use Eq. (38) along with the entropic uncertainty relations to bound the smooth min-entropy of the raw key register. Here the main difference

is the use of entropic chain rules to isolate the single-photon component of the raw key, before applying the EUR statement. In the second part, we use the obtained bound to prove the variable-length security statement. Here the main difference is due to to the presence of the $n_{K,1}$ in the event $\Omega_{(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\text{obs}}_{X,\mu_{\vec{k}}},e^{\text{obs}}_{Z},n_{K,0},n_{K,1})} = \widetilde{\Omega}$, which is handled differently. Let us first focus on the event $\Omega_{(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\text{obs}}_{X,\mu_{\vec{k}}},e^{\text{obs}}_{Z},n_{K,0},n_{K,1})} = \widetilde{\Omega}$. (In the remainder of this proof, we identify $\widetilde{\Omega} = \Omega_{(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\text{obs}}_{X,\mu_{\vec{k}}},e^{\text{obs}}_{Z},n_{K,1})}$ for brevity.)

F.0.1 Bounding the smooth min entropy

Similar to the proof of Theorem 1, we will use $\kappa(\widetilde{\Omega})$, to denote the probability of our computed bounds failing conditioned on the event $\widetilde{\Omega}$. We will see that the events that we will need to condition on are given by $\Omega_{(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\text{obs}}_{X,\mu_{\vec{k}}},e^{\text{obs}}_{Z},n_{K,1})}$. Even though we do not have access to the value $n_{K,1}$, we will see that this is the "right" event to condition on. We do not generate key from the zero-photon component $n_{K,0}$, since it has little impact on key rates for typical use cases. To see how one may do so, see Remark 21. As in Section B, we define

$$\begin{aligned}&\kappa(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\text{obs}}_{X,\mu_{\vec{k}}},e^{\text{obs}}_{Z},n_{K,1}) = \kappa(\widetilde{\Omega}) \coloneqq \\ &\Pr\Big(\boldsymbol{e^{\text{key}}_{X,1}} \geq \mathcal{B}_e(e^{\text{obs}}_{X,\mu_{\vec{k}}},n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}}) \quad \vee \quad \boldsymbol{n_{K,1}} \leq \mathcal{B}_1(n_{K,\mu_{\vec{k}}})\Big)_{\Omega_{(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\text{obs}}_{X,\mu_{\vec{k}}},e^{\text{obs}}_{Z},n_{K,1})}},\end{aligned} \tag{104}$$

which when combined with Eq. (38) implies

$$\sum_{n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\text{obs}}_{X,\mu_{\vec{k}}},e^{\text{obs}}_{Z},n_{K,1}} \Pr\Big(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\text{obs}}_{X,\mu_{\vec{k}}},e^{\text{obs}}_{Z},n_{K,1}\Big)\kappa(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\text{obs}}_{X,\mu_{\vec{k}}},e^{\text{obs}}_{Z},n_{K,1}) \leq \varepsilon^2_{\text{AT}}. \tag{105}$$

Thus, the average probability of *either* of our bounds failing (for any attack undertaken by Eve) is small.

The state prior to the final (third step) measurements by Alice and Bob, is given by $\rho_{A^{n_K}B^{n_K}E^nC^n|\widetilde{\Omega}}$. Suppose Alice measures her n_K systems in the Z basis. Let the post-measurement state be given by $\rho_{Z^{n_K}B^{n_K}E^nC^n|\widetilde{\Omega}}$. This state actually exists in the protocol, and we want to compute the smooth min entropy on this state. Instead of Z measurements, suppose Alice measures (virtually) in the X basis. In this case, let the post-measurement state be given by $\rho^{\text{virt}}_{X_A^{n_K}B^{n_K}E^nC^n|\widetilde{\Omega}}$. Since we condition on a specific value of $n_{K,1}$ in $\widetilde{\Omega}$, we can split up Z^{n_K} as $Z^{n_{K,1}}Z^{\text{rest}}$. The registers before measurements (A^{n_K}), and the X basis measurement registers ($X_A^{n_K}$) can also be split up in the same way.

Then, the required bound can be obtained via the following inequalities

$$\begin{aligned}H^{\sqrt{\kappa(\widetilde{\Omega})}}_{\min}(Z^{n_K}|C^nE^n)_{\rho|\widetilde{\Omega}} &\geq H^{\sqrt{\kappa(\widetilde{\Omega})}}_{\min}(Z^{n_{K,1}}|C^nE^n)_{\rho|\widetilde{\Omega}} \\ &\geq n_{K,1} - H^{\sqrt{\kappa(\widetilde{\Omega})}}_{\max}(X_A^{n_{K,1}}|B^{n_K})_{\rho|\widetilde{\Omega}} \\ &\geq n_{K,1}\left(1 - \mathcal{B}_e\left(h(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\text{obs}}_{X,\mu_{\vec{k}}},e^{\text{obs}}_{Z})\right)\right)\end{aligned} \tag{106}$$

where we used [62, Lemma 6.7] to isolate the single-photon contribution to the key in the first inequality, and the entropic uncertainty relations [1] followed by the same series of steps as in the proof of Theorem 1 to replace the smooth max entropy term with the bound on the phase error rate. This is the required bound on the smooth min entropy of the raw key.

Remark 21. If one wishes to obtain key from multi-photon or zero-photon events, one can use a suitable chain rule on the smooth min entropy at this stage (as is done in [35]). However, note that one must first fix the number of pulses corresponding to these events in order to have the registers be well-defined. For instance, one cannot apply the above analysis for a state ρ *without* conditioning on a $\widetilde{\Omega}$, since a fixed value of $n_{K,1}$ is required to meaningfully define the register $Z^{n_{K,1}}$.

This subtlety is missing in [35]. While one may choose to define these registers to store strings of variable length, this then complicates the application of EUR in the proof (since the number of rounds on which the EUR is applied is now variable). Our analysis is one rigorous way to avoid these problems.

We will now use Eq. (106) to prove the $(2\varepsilon_{\mathrm{AT}} + \varepsilon_{\mathrm{PA}})$-secrecy of the QKD protocol. To obtain $(2\varepsilon_{\mathrm{AT}} + \varepsilon_{\mathrm{PA}})$-secrecy, we must show that Eq. (73) is true. Again, as in the proof of Theorem 1, the states conditioned on $\widetilde{\Omega} = \Omega(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{X,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{Z}, n_{K,1}) \wedge \Omega_{\mathrm{EV}}$ have orthogonal supports. Therefore, it is enough to show that

$$\Delta := \frac{1}{2} \sum_{n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{X,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{Z}, n_{K,1}} \Pr\left(\widetilde{\Omega} \wedge \Omega_{\mathrm{EV}}\right) d(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{X,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{Z}, n_{K,1}) \leq 2\varepsilon_{\mathrm{AT}} + \varepsilon_{\mathrm{PA}},$$

$$d(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{X,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{Z}, n_{K,1}) := \left\| \rho_{K_A C^n C_E C_P E^n | \widetilde{\Omega} \wedge \Omega_{\mathrm{EV}}} - \sum_{k \in \{0,1\}^{l(\dots)}} \frac{|k\rangle\langle k|_{K_A}}{2^{l(\dots)}} \otimes \rho_{C^n C_E C_P E^n | \widetilde{\Omega} \wedge \Omega_{\mathrm{EV}}} \right\|_1 \tag{107}$$

since we can group together terms with the same output key to obtain Eq. (73) from Eq. (107) (and $l(\dots) = l(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{X,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{Z})$ for brevity). We will now prove Eq. (107). First, we split the sum over $n_{K,1}$ into two parts, depending on whether it satisfies our estimates from Eq. (38). Thus, we obtain

$$\begin{aligned}
\Delta &= \frac{1}{2} \sum_{\substack{n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{X,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{Z} \\ n_{K,1} > \mathcal{B}_1(n_{K,\mu_{\vec{k}}})}} \Pr\left(\widetilde{\Omega} \wedge \Omega_{\mathrm{EV}}\right) d(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{X,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{Z}, n_{K,1}) \\
&+ \frac{1}{2} \sum_{\substack{n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{X,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{Z} \\ n_{K,1} \leq \mathcal{B}_1(n_{K,\mu_{\vec{k}}})}} \Pr\left(\widetilde{\Omega} \wedge \Omega_{\mathrm{EV}}\right) d(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{X,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{Z}, n_{K,1}) \\
&= \Delta_1 + \Delta_2
\end{aligned} \tag{108}$$

Using the fact that $d(.) \leq 2$, the second term (Δ_2) can be upper bounded via

$$\Delta_2 \leq \sum_{\substack{n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{X,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{Z} \\ n_{K,1} \leq \mathcal{B}_1(n_{K,\mu_{\vec{k}}})}} \Pr\left(\widetilde{\Omega}\right) = \Pr\left(\boldsymbol{n_{K,1}} \leq \mathcal{B}_1(\boldsymbol{n_{K,\mu_{\vec{k}}}})\right) \tag{109}$$

The first term (Δ_1) can be bounded in an *identical* manner as in the proof of Theorem 1, we shown below. Again, we can assume that we are summing over events that lead to a non-trivial length of the key (since events where the protocol aborts do not contribute to Δ). Let $\mathcal{F} = \{(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{X,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{Z}) | l(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{X,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{Z}) > 0\}$ be the set of parameters that produce a non-trivial length of the key. Then, we obtain the following set of inequalities, which we

explain below:

$$
\begin{aligned}
\Delta_1 &\leq \sum_{\substack{n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\mathrm{obs}}_{X,\mu_{\vec{k}}},e^{\mathrm{obs}}_{Z}\in\mathcal{F} \\ n_{K,1}>\mathcal{B}_1(n_{K,\mu_{\vec{k}}})}} \Pr\left(\widetilde{\Omega}\right)\left(2\sqrt{\kappa(\widetilde{\Omega})}+\frac{1}{2}2^{-\frac{1}{2}\left(H_{\min}^{\sqrt{\kappa(\widetilde{\Omega})}}(Z^{n_K}|E^nC^nC_E)_{(\rho|\widetilde{\Omega})\wedge\Omega_{\mathrm{EV}}}-l(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\mathrm{obs}}_{X,\mu_{\vec{k}}},e^{\mathrm{obs}}_{Z})\right)}\right) \\
&\leq \sum_{\substack{n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\mathrm{obs}}_{X,\mu_{\vec{k}}},e^{\mathrm{obs}}_{Z}\in\mathcal{F} \\ n_{K,1}>\mathcal{B}_1(n_{K,\mu_{\vec{k}}})}} \Pr\left(\widetilde{\Omega}\right)\left(2\sqrt{\kappa(\widetilde{\Omega})}+\frac{1}{2}2^{-\frac{1}{2}\left(H_{\min}^{\sqrt{\kappa(\widetilde{\Omega})}}(Z^{n_K}|E^nC^nC_E)_{\rho|\widetilde{\Omega}}-l(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\mathrm{obs}}_{X,\mu_{\vec{k}}},e^{\mathrm{obs}}_{Z})\right)}\right) \\
&\leq \sum_{\substack{n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\mathrm{obs}}_{X,\mu_{\vec{k}}},e^{\mathrm{obs}}_{Z}\in\mathcal{F} \\ n_{K,1}>\mathcal{B}_1(n_{K,\mu_{\vec{k}}})}} \Pr\left(\widetilde{\Omega}\right)\left(2\sqrt{\kappa(\widetilde{\Omega})}\right. \\
&\quad \left.+\frac{1}{2}2^{-\frac{1}{2}\left(H_{\min}^{\sqrt{\kappa(\widetilde{\Omega})}}(Z^{n_K}|E^nC^n)_{\rho|\widetilde{\Omega}}-l(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\mathrm{obs}}_{X,\mu_{\vec{k}}},e^{\mathrm{obs}}_{Z}-\lambda_{\mathrm{EC}}(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\mathrm{obs}}_{X,\mu_{\vec{k}}},e^{\mathrm{obs}}_{Z})-\log(2/\varepsilon_{\mathrm{EV}})\right)}\right)\right) \\
&\leq \sum_{\substack{n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\mathrm{obs}}_{X,\mu_{\vec{k}}},e^{\mathrm{obs}}_{Z}\in\mathcal{F} \\ n_{K,1}>\mathcal{B}_1(n_{K,\mu_{\vec{k}}})}} \Pr\left(\widetilde{\Omega}\right)\left(2\sqrt{\kappa(\widetilde{\Omega})}\right. \\
&\quad \left.+\frac{1}{2}2^{-\frac{1}{2}\left(n_{K,1}\left(1-h\left(\mathcal{B}_e\left(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\mathrm{obs}}_{X,\mu_{\vec{k}}},e^{\mathrm{obs}}_{Z}\right)\right)\right)-l(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\mathrm{obs}}_{X,\mu_{\vec{k}}},e^{\mathrm{obs}}_{Z})-\lambda_{\mathrm{EC}}(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\mathrm{obs}}_{X,\mu_{\vec{k}}},e^{\mathrm{obs}}_{Z})-\log(2/\varepsilon_{\mathrm{EV}})\right)}\right)\right) \\
&= \sum_{\substack{n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\mathrm{obs}}_{X,\mu_{\vec{k}}},e^{\mathrm{obs}}_{Z}\in\mathcal{F} \\ n_{K,1}>\mathcal{B}_1(n_{K,\mu_{\vec{k}}})}} \Pr\left(\widetilde{\Omega}\right)\left(2\sqrt{\kappa(\widetilde{\Omega})}+\varepsilon_{\mathrm{PA}}\right) \\
&\leq \varepsilon_{\mathrm{PA}}+2\sqrt{\sum_{\substack{n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\mathrm{obs}}_{X,\mu_{\vec{k}}},e^{\mathrm{obs}}_{Z} \\ n_{K,1}>\mathcal{B}_1(n_{K,\mu_{\vec{k}}})}} \Pr\left(\widetilde{\Omega}\right)\kappa(\widetilde{\Omega})} \\
&= \varepsilon_{\mathrm{PA}}+2\sqrt{\Pr\left(\boldsymbol{e}^{\mathrm{key}}_{\boldsymbol{X,1}}\geq\mathcal{B}_e(\boldsymbol{e}^{\mathrm{obs}}_{\boldsymbol{X,\mu_{\vec{k}}}},\boldsymbol{n_{X,\mu_{\vec{k}}}},\boldsymbol{n_{K,\mu_{\vec{k}}}})\quad\wedge\quad\boldsymbol{n_{K,1}}>\mathcal{B}_1(\boldsymbol{n_{K,\mu_{\vec{k}}}})\right)}.
\end{aligned}
\tag{110}
$$

Here, we used the leftover-hashing lemma [2, Proposition 9] on the sub-normalized state $(\rho_{|\widetilde{\Omega}})_{\wedge\Omega_{\mathrm{EV}}}$ for the first inequality, and [2, Lemma 10] to get rid of the sub-normalized conditioning $(\wedge\Omega_{\mathrm{EV}})$ in the smooth min entropy term in the second inequality. We used [62, Lemma 6.8] to split off the error-correction information $(\lambda_{\mathrm{EC}}(n_{X,\mu_{\vec{k}}},n_{K,\mu_{\vec{k}}},e^{\mathrm{obs}}_{X,\mu_{\vec{k}}},e^{\mathrm{obs}}_{Z}))$ and error-verification information $(\log(2/\varepsilon_{\mathrm{EV}}))$ in the third inequality. We used the bound on the smooth min entropy from Eq. (106) for the fourth inequality. The fifth equality follows by replacing the values of $l(n_X,n_K,e^{\mathrm{obs}}_X,e^{\mathrm{obs}}_Z)$ and $\lambda_{\mathrm{EC}}(n_X,n_K,e^{\mathrm{obs}}_X,e^{\mathrm{obs}}_Z)$ from Eq. (53). We use the concavity of the square root function and Jensen's inequality for the sixth inequality to pull the sum over the events and the probability inside the square root, while the seventh equality follows simply from the definition of conditional probabilities and κ (Eq. (104)).

Combining our bounds on Δ_1 and Δ_2 from Eqs. (109) and (110), we obtain

$$\begin{aligned}
\Delta &\leq \varepsilon_{\mathrm{PA}} + 2\sqrt{\Pr\Big(\boldsymbol{e}^{\mathrm{key}}_{\boldsymbol{X},\boldsymbol{1}} \geq \mathcal{B}_e(\boldsymbol{e}^{\mathrm{obs}}_{\boldsymbol{X},\boldsymbol{\mu}_{\vec{k}}}, \boldsymbol{n}_{\boldsymbol{X},\boldsymbol{\mu}_{\vec{k}}}, \boldsymbol{n}_{\boldsymbol{K},\boldsymbol{\mu}_{\vec{k}}}) \quad \wedge \quad \boldsymbol{n}_{\boldsymbol{K},\boldsymbol{1}} \geq \mathcal{B}_1(\boldsymbol{n}_{\boldsymbol{K},\boldsymbol{\mu}_{\vec{k}}})\Big)} + \Pr\big(\boldsymbol{n}_{\boldsymbol{K},\boldsymbol{1}} \leq \mathcal{B}_1(\boldsymbol{n}_{\boldsymbol{K},\boldsymbol{\mu}_{\vec{k}}})\big) \\
&\leq \varepsilon_{\mathrm{PA}} + 2\sqrt{\Pr\Big(\boldsymbol{e}^{\mathrm{key}}_{\boldsymbol{X},\boldsymbol{1}} \geq \mathcal{B}_e(\boldsymbol{e}^{\mathrm{obs}}_{\boldsymbol{X},\boldsymbol{\mu}_{\vec{k}}}, \boldsymbol{n}_{\boldsymbol{X},\boldsymbol{\mu}_{\vec{k}}}, \boldsymbol{n}_{\boldsymbol{K},\boldsymbol{\mu}_{\vec{k}}}) \quad \wedge \quad \boldsymbol{n}_{\boldsymbol{K},\boldsymbol{1}} \geq \mathcal{B}_1(\boldsymbol{n}_{\boldsymbol{K},\boldsymbol{\mu}_{\vec{k}}})\Big)} + \Pr\big(\boldsymbol{n}_{\boldsymbol{K},\boldsymbol{1}} \leq \mathcal{B}_1(\boldsymbol{n}_{\boldsymbol{K},\boldsymbol{\mu}_{\vec{k}}})\big) \\
&= \varepsilon_{\mathrm{PA}} + 2\sqrt{\Pr\Big(\boldsymbol{e}^{\mathrm{key}}_{\boldsymbol{X},\boldsymbol{1}} \geq \mathcal{B}_e(\boldsymbol{e}^{\mathrm{obs}}_{\boldsymbol{X},\boldsymbol{\mu}_{\vec{k}}}, \boldsymbol{n}_{\boldsymbol{X},\boldsymbol{\mu}_{\vec{k}}}, \boldsymbol{n}_{\boldsymbol{K},\boldsymbol{\mu}_{\vec{k}}}) \quad \vee \quad \boldsymbol{n}_{\boldsymbol{K},\boldsymbol{1}} \leq \mathcal{B}_1(\boldsymbol{n}_{\boldsymbol{K},\boldsymbol{\mu}_{\vec{k}}})\Big)} \\
&\leq \varepsilon_{\mathrm{PA}} + 2\varepsilon_{\mathrm{AT}}.
\end{aligned} \tag{111}$$

Here we use the fact that $2\sqrt{a}+b \leq 2\sqrt{a+b}$ for $0 \leq a, b, a+b \leq 1$ in the second inequality. We use $\Pr\big(\Omega_{(1)} \wedge \Omega^c_{(2)}\big) + \Pr\big(\Omega_{(2)}\big) = \Pr\big(\Omega_{(1)} \vee \Omega_{(2)}\big)$ (where Ω^c denotes the complement of Ω) for the third equality, and Eq. (38) for the final inequality.

□

Notice that our proofs of variable-length security (Theorems 1 and 3) rely on obtaining a suitable bound on the smooth min entropy of the raw key register, with a suitable smoothing parameter, for suitable events. In particular, the smoothing parameter averaged over all events satisfies certain bounds. However, the theorem statements so far have been specific to BB84 and decoy-state BB84. We state the following technical theorem regarding variable-length security which is applicable to generic protocols, as long as suitable bounds on the smooth min entropy can be obtained.

Theorem 4. In a QKD protocol, let $\Omega_{(i,j)}$ denote well-defined events (we use i for observed events and j for unobserved events) that can take place. Let $\vec{Z}$ denote the raw key register, let $\vec{E}$ denote Eve's quantum system, and let $\vec{C}$ denote public announcements (excluding error-correction and error-verification). Let the protocol be such that it produces a key of length $l(i)$ bits, using $\lambda_{\mathrm{EC}}(i)$ bits for error-correction and $\log(2/\varepsilon_{\mathrm{EV}})$ bits for error-verification, upon the observed event $\Omega_{(i)} \wedge \Omega_{\mathrm{EV}}$. For each i, let S_i denote a subset of possible values of j, and let $\kappa_{(i,j)} \geq 0$ be a set of values such that

$$\begin{aligned}
&H_{\min}^{\sqrt{\kappa_{(i,j)}}}(\vec{Z}|\vec{E}\vec{C})_{\rho|\Omega_{(i,j)}} \geq \beta_i \qquad\qquad \forall i, \forall j \in S_i \\
&\sum_i \sum_{j \in S_i} \Pr\big(\Omega_{(i,j)}\big)\kappa_{(i,j)} + \sum_i \sum_{j \notin S_i} \Pr\big(\Omega_{(i,j)}\big) \leq \varepsilon_{\mathrm{AT}}^2 \\
&l(i) \coloneqq \max\big\{\beta_i - \lambda_{\mathrm{EC}}(i) - 2\log(1/2\varepsilon_{\mathrm{PA}}) - \log(2/\varepsilon_{\mathrm{PA}}), 0\big\}.
\end{aligned} \tag{112}$$

Then the QKD protocol is $(2\varepsilon_{\mathrm{AT}} + \varepsilon_{\mathrm{PA}} + \varepsilon_{\mathrm{EV}})$-secure.

Proof Sketch. The proof follows an identical series of steps as the proof of Theorem 3, and we do not repeat it here. This can be seen by identifying i with observed events in the protocol (analogous to $(n_{X,\mu_{\vec{k}}}, n_{K,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{X,\mu_{\vec{k}}}, e^{\mathrm{obs}}_{Z})$), and j with events that are not directly observed in the protocol (analogous to $n_{K,1}$). One identifies the set S_i with values of j that satisfy certain bounds with high probability.

Intuitively the conditions in Eq. (112) split all possible combinations of (i,j) into two sets, depending on whether $j \in S_i$ or $j \notin S_i$. If $j \in S_i$, then a suitable bound β_i on the min entropy is known. This bound is utilized in the leftover hash lemma, and the trace distance for QKD security is bounded in the same manner as Eq. (110). The bound obtained in this case is given by $\varepsilon_{\mathrm{PA}} + 2\sqrt{\sum_{i,j\in S_i} \Pr\big(\Omega_{(i,j)}\big)\kappa_{(i,j)}}$. If $j \notin S_i$, then the trace distance for QKD security is bounded in the same manner as Eq. (109). The bound obtained is given by $\sum_{i,j\notin S_i} \Pr\big(\Omega_{(i,j)}\big)$. These two bounds can be combined as in Eq. (111).

Note that if j is set to be a trivial value, then given the suitable bound on the min entropy, we recover Theorem 1.

In general, when dealing with events, one must ensure that all events considered are well-defined, i.e, there exists (in theory) a classical register that determines whether the event occured or did not occur [2, Section 2].

G Detector Model Calculations

In this section we will compute upper bounds on the δ_1, δ_2. To do so, we follow the recipe from Section 6.1.

G.1 Computing POVMs

Recall that Alice and Bob's joint POVM $\{\Gamma_{(b_A,b_B),(\neq)}, \Gamma_{(b_A,b_B),(=)}, \Gamma_{(b_A,b_B),(\perp)}\}$ is given in Eq. (58). We can choose

$$\begin{aligned}
\tilde{F} &= \mathrm{I}_A \otimes \sum_{N_0,N_1=0}^{\infty} \left(1-(1-d_{\max})^2(1-\eta_{\max})^{N_0+N_1}\right) |N_0,N_1\rangle\langle N_0,N_1|_Z \\
&= \mathrm{I}_A \otimes \sum_{N_0,N_1=0}^{\infty} \left(1-(1-d_{\max})^2(1-\eta_{\max})^{N_0+N_1}\right) |N_0,N_1\rangle\langle N_0,N_1|_X\,, \quad \text{where} \\
\eta_{\max} &= \max_{b\in\{X,Z\}} \{\eta_{b_0},\eta_{b_1}\}, \quad \text{and } d_{\min} = \min_{b\in\{X,Z\}} \{d_{b_0},d_{b_1}\}, \\
\eta_{\min} &= \min_{b\in\{X,Z\}} \{\eta_{b_0},\eta_{b_1}\}, \quad \text{and } d_{\max} = \max_{b\in\{X,Z\}} \{d_{b_0},d_{b_1}\}.
\end{aligned} \tag{113}$$

It is straightforward to verify that $\tilde{F}$ satisfies our requirement $\tilde{F} \geq \Gamma_{(b_A,b_B),(\neq)} + \Gamma_{(b_A,b_B),(=)} = \mathrm{I} - \Gamma_{(b_A,b_B),(\perp)}$ for all choices of b_A, b_B. Then, we calculate the POVM elements from Eq. (55) as

$$\begin{aligned}
F_{(b),(\mathrm{con})} &= \mathrm{I}_A \otimes \sum_{N_0,N_1=0}^{\infty} \frac{1-(1-d_{b_0})(1-d_{b_1})(1-\eta_{b_0})^{N_0}(1-\eta_{b_1})^{N_1}}{(1-(1-d_{\max})^2(1-\eta_{\max})^{N_0+N_1})} |N_0,N_1\rangle\langle N_0,N_1|_b \\
F_{(b),(\perp)} &= \mathrm{I}_A \otimes \sum_{N_0,N_1=0}^{\infty} \left(1 - \frac{1-(1-d_{b_0})(1-d_{b_1})(1-\eta_{b_0})^{N_0}(1-\eta_{b_1})^{N_1}}{(1-(1-d_{\max})^2(1-\eta_{\max})^{N_0+N_1})}\right) |N_0,N_1\rangle\langle N_0,N_1|_b \\
G^{\mathrm{con}}_{(b),(\neq)} &= \sum_{N_0,N_1=0}^{\infty} |0\rangle\langle 0|_b \otimes \frac{(1+(1-d_{b_0})(1-\eta_{b_0})^{N_0})(1-(1-d_{b_1})(1-\eta_{b_1})^{N_1})}{2(1-(1-d_{b_0})(1-d_{b_1})(1-\eta_{b_0})^{N_0}(1-\eta_{b_1})^{N_1})} |N_0,N_1\rangle\langle N_0,N_1|_b \\
&\quad + |1\rangle\langle 1|_b \otimes \frac{(1+(1-d_{b_1})(1-\eta_{b_1})^{N_1})(1-(1-d_{b_0})(1-\eta_{b_0})^{N_0})}{2(1-(1-d_{b_0})(1-d_{b_1})(1-\eta_{b_0})^{N_0}(1-\eta_{b_1})^{N_1})} |N_0,N_1\rangle\langle N_0,N_1|_b \\
G^{\mathrm{con}}_{(b),(=)} &= \sum_{N_0,N_1=0}^{\infty} |0\rangle\langle 0|_b \otimes \frac{(1+(1-d_{b_1})(1-\eta_{b_1})^{N_1})(1-(1-d_{b_0})(1-\eta_{b_0})^{N_0})}{2(1-(1-d_{b_0})(1-d_{b_1})(1-\eta_{b_0})^{N_0}(1-\eta_{b_1})^{N_1})} |N_0,N_1\rangle\langle N_0,N_1|_b \\
&\quad + |1\rangle\langle 1|_b \otimes \frac{(1+(1-d_{b_0})(1-\eta_{b_0})^{N_0})(1-(1-d_{b_1})(1-\eta_{b_1})^{N_1})}{2(1-(1-d_{b_0})(1-d_{b_1})(1-\eta_{b_0})^{N_0}(1-\eta_{b_1})^{N_1})} |N_0,N_1\rangle\langle N_0,N_1|_b\,.
\end{aligned} \tag{114}$$

G.2 Computing δ_1

To compute the costs in Eq. (56), we first note that all POVMs appearing in this work are block-diagonal in the total photon number $N_0 + N_1$. We wish to compute the infinity norm, i.e

$$\delta_1 = 2\left\| \sqrt{F_{(Z),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty .$$

Due to block-diagonal structure, the operator appearing inside the $\|.\|_\infty$ in the above expressions are also block-diagonal in photon number $N_0 + N_1$. From the properties of the norm, we have that

$$\delta_1 = \max_N \delta_1^{(N)}, \tag{115}$$

where $\delta_1^{(N)}$ is the infinity norm for the block corresponding to total photon number $N = N_0 + N_1$. We now focus on computing $\delta_1^{(N)}$.

First, we compute $\delta_1^{(0)}$ directly as

$$\begin{aligned}
\frac{\delta_1^{(0)}}{2} =& \left\| \mathrm{I}_A \otimes |0,0\rangle\langle 0,0| \left(\sqrt{F_{(Z),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(X),(\mathrm{con})}} \right) \mathrm{I}_A \otimes |0,0\rangle\langle 0,0| \right\|_\infty \\
=& \left| \frac{1-(1-d_{Z_0})(1-d_{Z_1})}{1-(1-d_{\max})^2} - \frac{1-(1-d_{X_0})(1-d_{X_1})}{1-(1-d_{\max})^2} \right| \\
& \times \max\left\{ \frac{d_{X_1}(2-d_{X_0})}{2(1-(1-d_{X_0})(1-d_{X_1}))}, \frac{d_{X_0}(2-d_{X_1})}{2(1-(1-d_{X_0})(1-d_{X_1}))} \right\} \\
=& \left| \frac{(1-d_{X_0})(1-d_{X_1}) - (1-d_{Z_0})(1-d_{Z_1})}{1-(1-d_{\max})^2} \right| \max\left\{ \frac{d_{X_1}(2-d_{X_0})}{2(1-(1-d_{X_0})(1-d_{X_1}))}, \frac{d_{X_0}(2-d_{X_1})}{2(1-(1-d_{X_0})(1-d_{X_1}))} \right\} \\
\leq& \left(1 - \frac{1-(1-d_{\min})^2}{1-(1-d_{\max})^2} \right) \frac{d_{\max}(2-d_{\min})}{2(1-(1-d_{\min})^2)}. \qquad (116)
\end{aligned}$$

To bound $\delta_1^{(N)}$ for $N \neq 0$, we write

$$\begin{aligned}
\frac{\delta_1}{2} =& \left\| \sqrt{F_{(Z),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty \\
\leq& \left\| \sqrt{F_{(Z),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(Z),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty \\
& + \left\| \sqrt{F_{(Z),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(X),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty \qquad (117) \\
\leq& \left\| \sqrt{F_{(Z),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \right\|_\infty \left\| \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty \\
& + \left\| \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty \left\| G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty, \qquad (118)
\end{aligned}$$

where Eq. (117) follows from the triangle inequality, and Eq. (118) follows from the submultiplicativity of the ∞-norm. We can then compute each term individually. Note that due to the submultiplicativity of the ∞-norm, we have

$$\left\| \sqrt{F_{(b),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \right\|_\infty \leq \left\| \sqrt{F_{(b),(\mathrm{con})}} \right\|_\infty \left\| G^{\mathrm{con}}_{(X),(\neq)} \right\|_\infty \leq 1. \qquad (119)$$

Thus, we only need to bound $\left\| \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty$. To do so, we define

$$\begin{aligned}
P :=& \mathrm{I}_A \otimes \sum_{N=0}^{\infty} \sum_{N_0+N_1=N} \frac{\sqrt{1-(1-d_{\max})^2(1-\eta_{\max})^N} + \sqrt{1-(1-d_{\min})^2(1-\eta_{\min})^N}}{2\sqrt{1-(1-d_{\max})^2(1-\eta_{\max})^N}} |N_0,N_1\rangle\langle N_0,N_1|_X \\
=& \mathrm{I}_A \otimes \sum_{N=0}^{\infty} \sum_{N_0+N_1=N} \frac{\sqrt{1-(1-d_{\max})^2(1-\eta_{\max})^N} + \sqrt{1-(1-d_{\min})^2(1-\eta_{\min})^N}}{2\sqrt{1-(1-d_{\max})^2(1-\eta_{\max})^N}} |N_0,N_1\rangle\langle N_0,N_1|_Z , \qquad (120)
\end{aligned}$$

and obtain

$$\left\| \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty \leq \left\| \sqrt{F_{(Z),(\mathrm{con})}} - P \right\|_\infty + \left\| P - \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty, \qquad (121)$$

where Eq. (121) is a consequence of the triangle inequality. Let us focus on a fixed value of $N = N_0 + N_1 \neq 0$. In this case, combining Eqs. (118), (119) and (121) allows us to obtain

$$\begin{aligned}
\delta_1^{(N)} \leq& 4 \sum_{b=X,Z} \left| \sqrt{\frac{1-(1-d_{b_0})(1-d_{b_1})(1-\eta_{b_0})^{N_0}(1-\eta_{b_1})^{N_1}}{1-(1-d_{\max})^2(1-\eta_{\max})^{N_0+N_1}}} \right. \\
& \left. - \frac{\sqrt{1-(1-d_{\max})^2(1-\eta_{\max})^{N_0+N_1}} + \sqrt{1-(1-d_{\min})^2(1-\eta_{\min})^{N_0+N_1}}}{2\sqrt{1-(1-d_{\max})^2(1-\eta_{\max})^{N_0+N_1}}} \right| \qquad (122) \\
\leq& 4 \left| 1 - \sqrt{\frac{1-(1-d_{\min})^2(1-\eta_{\min})^N}{1-(1-d_{\max})^2(1-\eta_{\max})^N}} \right|,
\end{aligned}$$

where the final inequality above follows from the monotonicity of the expression inside the modulus with respect to $\eta_{b_0}, \eta_{b_1}, d_{b_0}, d_{b_1}$. However, as described in Ref. [53, Section III C] we can renormalize detection efficiencies and treat the common loss in detectors as part of the channel. Thus, without loss of generality, we consider one of the detectors to be lossless. This can be thought of as setting $\eta_{\max} \to 1$ and $\eta_{\min} \to \eta_{\min}/\eta_{\max}$. This significantly simplifies the calculations. Combining Eqs. (115), (117), (119), (121) and (122), we obtain

$$\delta_1^{(N)} \leq 4\left|1 - \sqrt{1-(1-d_{\min})^2(1-r_\eta)^N}\right|, \qquad (N \geq 1) \tag{123}$$

Combining Eqs. (116) and (123), we obtain

$$\delta_1 \leq \max\left\{\left(1 - \frac{1-(1-d_{\min})^2}{1-(1-d_{\max})^2}\right)\frac{d_{\max}(2-d_{\min})}{1-(1-d_{\min})^2}, 4\left|1-\sqrt{1-(1-d_{\min})^2(1-r_\eta)}\right|\right\}, \tag{124}$$

where $r_\eta = \eta_{\min}/\eta_{\max}$.

G.3 Computing δ_2

We can now also compute $\delta_2 = \left\|\mathrm{I} - F_{(Z),(\mathrm{con})}\right\|_\infty$ in a similar way, using Eqs. (56) and (114). Again, we have $\delta_2 = \max_N \delta_2^{(N)}$, where

$$\begin{aligned}\delta_2^{(N)} &= \max_{N_0+N_1=N}\left\{1 - \frac{1-(1-d_{Z_0})(1-d_{Z_1})(1-\eta_{Z_0})^{N_0}(1-\eta_{Z_1})^{N_1}}{1-(1-d_{\max})^2(1-\eta_{\max})^N}\right\} \\ &\leq \max_{N_0+N_1=N}\left\{1 - \frac{1-(1-d_{\min})^2(1-\eta_{\min})^N}{1-(1-d_{\max})^2(1-\eta_{\max})^N}\right\},\end{aligned} \tag{125}$$

where the second inequality follows from the fact that the term inside is monotonous with respect to $\eta_{Z_0}, \eta_{Z_1}, d_{Z_0}, d_{Z_1}$. As in the computation for δ_1, we pull out common loss by setting $\eta_{\max} \to 1$, $\eta_{\min} \to \eta_{\min}/\eta_{\max}$. Using Eq. (125), δ_2 can be bounded as

$$\delta_2 \leq \max\left\{1 - \frac{1-(1-d_{\min})^2}{1-(1-d_{\max})^2}, (1-d_{\min})^2(1-r_\eta)\right\}, \tag{126}$$

where $r_\eta = \eta_{\min}/\eta_{\max}$.

H Random Swapping

We compute δ_1, δ_2 for the scenario where random swapping is implemented with probability $p = 1/2$. Bob's POVM elements are given as in Eq. (63).

Note in particular that the zero-photon and single-photon component of $\Gamma_{(b,\perp)}^{(B),(\mathrm{swap})}$ is independent of the basis choice b. Thus, we can choose

$$\begin{aligned}\tilde{F} &= \mathrm{I}_A \otimes (1-(1-d_{\mathrm{mult}})^2)\,|0,0\rangle\langle 0,0| \\ &\quad + \mathrm{I}_A \otimes \left(1-(1-d_{\mathrm{mult}})^2(1-\eta_{\mathrm{avg}})\right)\left(|0,1\rangle\langle 0,1|_Z + |1,0\rangle\langle 1,0|_Z\right) \\ &\quad + \mathrm{I}_A \otimes \sum_{\substack{N_0,N_1=0 \\ N_0+N_1>1}}^{\infty} (1-(1-d_{\mathrm{mult}})^2(1-\eta_{\mathrm{mult}})^{N_0+N_1})\,|N_0,N_1\rangle\langle N_0,N_1|_Z\,, \quad \text{where} \\ \eta_{\mathrm{mult}} &= 1-\sqrt{(1-\eta_0)(1-\eta_1)}, \quad \text{and } d_{\mathrm{mult}} = 1-\sqrt{(1-d_0)(1-d_1)}, \\ \eta_{\mathrm{avg}} &= \frac{\eta_0+\eta_1}{2}, \quad \text{and } \eta_{\min} = \min\{\eta_0,\eta_1\},\end{aligned} \tag{127}$$

Note that replacing Z with X does not change the above expressions. This results in

$$
\begin{aligned}
F_{(b),(\mathrm{con})} &= \mathrm{I}_A \otimes |0,0\rangle\langle 0,0| \\
&\quad + \mathrm{I}_A \otimes (|0,1\rangle\langle 0,1|_b + |1,0\rangle\langle 1,0|_b) \\
&\quad + \mathrm{I}_A \otimes \sum_{\substack{N_0,N_1=0 \\ N_0+N_1>1}}^{\infty} \frac{2-(1-d_{\mathrm{mult}})^2\left((1-\eta_{b_0})^{N_0}(1-\eta_{b_1})^{N_1}+(1-\eta_{b_1})^{N_0}(1-\eta_{b_0})^{N_1}\right)}{2(1-(1-d_{\mathrm{mult}})^2(1-\eta_{\mathrm{mult}})^{N_0+N_1})} |N_0,N_1\rangle\langle N_0,N_1|_b \,.
\end{aligned} \tag{128}
$$

As a consequence of the way in which we bound the metrics δ_1 and δ_2, these are the only POVM elements we need to explicitly compute.

H.1 Computing δ_1

Similar to the analysis performed in Section G.2, we reduce the problem to bounding $\left\|\sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}}\right\|_\infty$ through Eqs. (118) and (119). Once again we exploit the block-diagonal structure in the POVM elements to compute the infinity norm $\delta_1^{(N)}$ of each block with total photon-number N separately as done in Eq. (115). First, note that $\delta_1^{(0)} = \delta_1^{(1)} = 0$. To compute $\delta^{(N)}$ for $N \geq 2$, we define

$$
\begin{aligned}
P &\coloneqq \mathrm{I}_A \otimes \sum_{N=2}^{\infty} \sum_{N_0+N_1=N} \frac{\sqrt{1-(1-d_{\mathrm{mult}})^2(1-\eta_{\mathrm{mult}})^N} + \sqrt{1-(1-d_{\mathrm{mult}})^2\frac{(1-\eta_0)^N+(1-\eta_1)^N}{2}}}{2\sqrt{1-(1-d_{\mathrm{mult}})^2(1-\eta_{\mathrm{mult}})^N}} |N_0,N_1\rangle\langle N_0,N_1|_X \\
&= \mathrm{I}_A \otimes \sum_{N=2}^{\infty} \sum_{N_0+N_1=N} \frac{\sqrt{1-(1-d_{\mathrm{mult}})^2(1-\eta_{\mathrm{mult}})^N} + \sqrt{1-(1-d_{\mathrm{mult}})^2\frac{(1-\eta_0)^N+(1-\eta_1)^N}{2}}}{2\sqrt{1-(1-d_{\mathrm{mult}})^2(1-\eta_{\mathrm{mult}})^N}} |N_0,N_1\rangle\langle N_0,N_1|_Z \,,
\end{aligned} \tag{129}
$$

and obtain

$$
\left\|\sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}}\right\|_\infty \leq \left\|\sqrt{F_{(Z),(\mathrm{con})}} - P\right\|_\infty + \left\|P - \sqrt{F_{(X),(\mathrm{con})}}\right\|_\infty, \tag{130}
$$

identically to Eq. (121).

Following a similar calculation as in Eq. (122), we obtain

$$
\delta_1^{(N)} \leq 4\left(1 - \sqrt{\frac{1-(1-d_{\mathrm{mult}})^2\frac{(1-\eta_0)^N+(1-\eta_1)^N}{2}}{1-(1-d_{\mathrm{mult}})^2(1-\eta_{\mathrm{mult}})^N}}\right), \tag{131}
$$

for all $N \geq 2$. Once again we use the argument in [53, Section III C] to treat the common loss in detectors as part of the channel. This is equivalent to setting $\eta_{\max} \to 1$ and $\eta_{\min} \to r_\eta = \eta_{\min}/\eta_{\max}$. (Actually this sets $\eta_{\mathrm{mult}} \to 1$ and one of η_i to 1 and the other to r_η). Thus we obtain

$$
\delta_1^{(N)} \leq 4\left(1 - \sqrt{1-(1-d_{\mathrm{mult}})^2\frac{(1-r_\eta)^N}{2}}\right). \tag{132}
$$

The above expression is monotonic in N. Therefore, we obtain

$$
\delta_1 \leq 4\left(1 - \sqrt{1-(1-d_{\mathrm{mult}})^2\frac{(1-r_\eta)^2}{2}}\right). \tag{133}
$$

H.2 Computing δ_2

We can also compute $\delta_2 = \left\|\mathrm{I} - F_{(Z),(\mathrm{con})}\right\|_\infty$ similarly to the computation in Section G.3. Again, we have $\delta_2 = \max_N \delta_2^{(N)}$. Similar to Section H.1 we obtain $\delta_2^{(0)} = \delta_2^{(1)} = 0$. A straightforward computation for the other blocks results in

$$
\delta_2 \leq (1-d_{\mathrm{mult}})^2\frac{(1-r_\eta)^2}{2}. \tag{134}
$$