


Imperfect phase randomization and generalized decoy-state quantum key distribution

Shlok Nahar^{✉,*}, Twesh Upadhyaya, and Norbert Lütkenhaus

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

 (Received 9 September 2023; revised 16 November 2023; accepted 1 December 2023; published 18 December 2023)

Decoy-state methods are essential to perform quantum key distribution (QKD) at large distances in the absence of single-photon sources. However, the standard techniques apply only if laser pulses are used that are independent and identically distributed. Moreover, they require that the laser pulses are fully phase randomized. However, realistic high-speed QKD setups do not meet these stringent requirements. In this work, we generalize decoy-state analysis to accommodate laser sources that emit imperfectly phase-randomized states. We also develop theoretical tools to prove the security of protocols with lasers that emit pulses that are independent, but not identically distributed. These tools can be used with recent work [G. Currás-Lorenzo, S. Nahar, N. Lütkenhaus, K. Tamaki, and M. Curty, *Quantum Sci. Technol.* (2023)] to prove the security of laser sources with correlated phase distributions as well. We quantitatively demonstrate the effect of imperfect phase randomization on key rates by computing the key rates for a simple implementation of the three-state protocol.

DOI: [10.1103/PhysRevApplied.20.064031](https://doi.org/10.1103/PhysRevApplied.20.064031)

I. INTRODUCTION

Quantum key distribution (QKD) is a method to realize quantum-safe cryptography [1]. Since QKD does not rely on computational assumptions, QKD protocols can be proved to be information-theoretically secure [2–4]. However, practical implementations suffer from security loopholes, which arise from a gap between the theoretic models for which security is proved, and the experimental devices that perform QKD [5]. Thus, better modeling of devices as well as theoretical tools to perform security analysis with these more detailed models is essential for the implementation security of QKD protocols.

There have been recent advances to theoretically accommodate general source imperfections [6–8]. However, these techniques cannot be used at present with the decoy-state method [9–11], which is essential to get secret key rates at large distances with coherent states. To this end, there has been more work on doing decoy-state QKD with intensity correlations [12,13].

Besides the absence of intensity correlations, standard decoy-state methods still assume that the laser outputs fully phase-randomized states. For phase randomization in gain-switched laser diodes, it is essential that no photons from previous pulses remain in the lasing cavity at the start of the next lasing [14]. However, as discussed in

Ref. [15], Eve could perform an active laser-seeding attack [16], which would invalidate such an assumption. Thus, we attempt to fill this security gap by proving the security for decoy-state protocols for a source that emits independent (i.e., noncorrelated) pulses whose phase is distributed nonuniformly.

Further, for lasers with a high repetition rate [17] there is not enough time for the laser cavity to empty out between pulses. In this case, the laser pulses might even have correlated phase distributions. Techniques to prove the security of decoy-state QKD in the presence of phase correlations were developed in Ref. [15], which crucially build on the tools described in this paper. Their proof technique reduces the security analysis of phase-correlated laser pulses to that of laser pulses that have an independent and nonidentically distributed phase distribution. The decoy-state analysis for such phase-independent states was described by one of the authors in Ref. [18]. Note that as shown in Ref. [15], the proof techniques described in Ref. [18] only work for laser pulses that have no phase correlations.

In Sec. III A, we develop tools to reduce the security of phase-independent laser pulses to the security of an independent identically distributed (IID) partially phase-randomized laser. For this reduction, the phase distribution of the laser pulses must be partially characterized by a single parameter. This is practically useful only if this parameter is experimentally measurable. So, we include a discussion on the methods and difficulties of measuring this quantity in Sec. III B.

*sanahar@uwaterloo.ca

In order to use decoy-state analysis for partially phase-randomized laser pulses, we draw an analogy with channel tomography to state our generalized decoy-state methods in Sec. IV. However, as outlined with the requisite background in Sec. II, a full decoy-state analysis in this approach requires the diagonalization of the laser states. Thus, we describe how to approximately diagonalize a density matrix in Sec. V. Additionally, we note that these methods are quite general with imperfect phase randomization being just one possible application.

In summary, we develop tools that enable us to perform decoy-state QKD with lasers that have imperfect phase randomization. We then use these tools to analyze the security of the three-state protocol with phase imperfections in Sec. VI as an example. We also plot our results to depict the effect of the phase imperfections for this protocol.

II. BACKGROUND

In this section we first summarize the steps in a generic prepare and measure (PM) protocol. We then review the key rate optimization problem, and discuss the concept of source maps, a proof technique used to find lower bounds on the key rate.

A. QKD protocol steps

Here we outline the steps in a generic PM protocol with n rounds. We focus in particular on the asymptotic limit, where the number of protocol rounds n tends to infinity.

(1) **State preparation:** Alice randomly prepares one of a set of quantum states $\{\rho_1^\mu \dots \rho_n^\mu\}$ with an *a priori* probability distribution $\{p(i, \mu)\}$, where the signal modulation i and signal intensity μ denote which state she chose. The prepared states are called signal (and decoy) states. We model Alice's signal preparation procedure as different channels acting on some fixed base state $\rho_i^\mu = \Xi_i(\rho^\mu)$. We denote the quantum system associated with each of these signal states A'_m for the m th round of the protocol.

(2) **Signal transmission:** Alice sends her prepared states to Bob via an insecure quantum channel

$$\mathcal{E} : A'_1 \dots A'_n \rightarrow B_1 \dots B_n$$

where each B_m denotes the quantum system associated with each of the states Bob receives in round m .

(3) **Measurement:** Bob measures the states that he receives by a k -outcome positive operator-valued measure (POVM) $\{\Gamma_j\}_{j=1}^k$ and records the outcome from each round.

After repeating the above steps multiple times, we proceed to the next part of the protocol.

(4) **Acceptance testing:** Alice and Bob randomly choose a subset of the rounds for testing. For the rounds

chosen for testing, they both publicly announce the signal modulation i and signal intensity μ chosen, and measurement outcome j to form a frequency distribution. They then check if this frequency distribution belongs to the acceptance set agreed upon before running the protocol. If it does, they proceed with the protocol after discarding the test results. Otherwise, they abort.

In the asymptotic limit, assuming that Eve's attack is IID, i.e., $\mathcal{E} = \Phi^{\otimes n}$, the frequency distribution converges to a probability distribution $p(i, \mu, j) = p(i, \mu) \text{Tr}[\Gamma_j \Phi(\rho_i^\mu)]$. This probability distribution effectively constrains Φ , and thus Eve's actions on the states that Alice sent Bob.

(5) **Announcements and sifting:** Alice and Bob make announcements over the authenticated classical channel. They sift the nontested data based on the announcements made, i.e., they choose a subset of signal and measurement data to keep and discard the rest based on the announcements.

(6) **Key map:** Alice uses her signal modulation data i as well as the announcements to map her data into a key string x . This is called the raw key. We assume here that the key is a bit string for simplicity, but all the steps can be applied more generally.

(7) **Error correction:** Alice and Bob then perform error correction over the authenticated classical channel to make Bob's measurement outcomes match with Alice's bit string x . We denote the data communicated per key bit to Eve in this process as δ_{leak} .

(8) **Privacy amplification:** Alice and Bob produce their final secret key by applying an appropriate hash function on the raw key (Theorem 5.5.1 of Ref. [19]).

PM protocols are typically implemented in experiments. However, it is easier to analyze the security of another class of protocols, entanglement-based (EB) protocols where Alice and Bob share an entangled bipartite state instead of step (1) of the PM protocol.

Fortunately, we can reduce the analysis of any PM protocol to the analysis of an EB protocol with added constraints via a source-replacement scheme [20–22] as follows. First, define $|\rho_i^\mu\rangle_{A_S A'}$ to be a purification of ρ_i^μ . The purifying system A_S , termed the shield system [23], is useful for the security proof if Alice sends Bob mixed states. Neither Alice nor Bob interacts with the shield system at any point.

Alice prepares the state

$$|\psi\rangle_{A_S A'} = \sum_{i, \mu} \sqrt{p(i, \mu)} |i, \mu\rangle_A \otimes |\rho_i^\mu\rangle_{A_S A'} \quad (1)$$

and sends system A' to Bob through the insecure quantum channel to get the state $\rho_{A_S B}$. In addition to the constraints from step (4) of the protocol that take the form $p(i, \mu, j) =$

$\text{Tr}[(|i, \mu\rangle\langle i, \mu|_A \otimes \mathbb{I}_{A_S} \otimes \Gamma_j) \rho_{AA_S B}]$, we get the constraint $\text{Tr}_B[\rho_{AA_S B}] = \text{Tr}'_A[|\psi\rangle\langle\psi|_{AA_S A'}]$. Intuitively, this represents the fact that Eve cannot change the states in Alice's lab and shield system, although she can act freely on the state sent to Bob. We shall now briefly outline how we can use these constraints to reliably lower bound the secret key rate that we can obtain from a QKD protocol.

B. Numerical asymptotic key rate

The secret key rate in the asymptotic limit under the IID assumption can be found using the Devetak-Winter formula: $R^\infty = H(Z|E) - \delta_{\text{leak}}$ where Z is the key register, E is Eve's register, and δ_{leak} is the number of bits per round leaked to Eve during step (7) of the protocol. A lower bound for the key rate can be found by minimizing the first term over all possible marginal states that Eve could hold. The Devetak-Winter key rate can be lifted to coherent attacks if the protocol is permutation invariant via the quantum de Finetti theorem [24] or the postselection technique [25].

Following Refs. [26,27], the Devetak-Winter key rate formula for an EB protocol can be reformulated as an SDP

$$\begin{aligned}
 R^\infty &= \min_{\rho_{AA_S B}} D(\mathcal{G}(\rho_{AA_S B}) \| \mathcal{Z}(\mathcal{G}(\rho_{AA_S B}))) - \delta_{\text{leak}} \\
 &\text{such that } \text{Tr}[\Gamma_j \Phi(\rho_i^\mu)] = \gamma_{j|i, \mu} \quad \forall i, j, \mu \\
 &\text{Tr}_B[\rho_{AA_S B}] = \rho_{AA_S},
 \end{aligned} \quad (2)$$

where A , A_S , and B are Alice and Bob's registers together with the shield system. The statistics $\gamma_{j|i, \mu}$ can be understood to be the conditional probability of Bob observing outcome j given that Alice sent signal state i and intensity μ . Here, the relative entropy $D(\mathcal{G}(\rho_{AA_S B}) \| \mathcal{Z}(\mathcal{G}(\rho_{AA_S B})))$ is the objective function where \mathcal{G} is a map that represents the protocol (including announcements), and \mathcal{Z} is a map that can be constructed from the key map.

Since we do not use most of the specific details of these maps, we abstract the objective function as $f(\rho_{AA_S B})$. For details, see Refs. [26,27]. Note that although $\rho_{AA_S B}$ contains all signal and decoy intensities μ , we choose to include only the signal intensity $\mu = \mu_S$ in the objective function for computational simplicity by using a key map that assigns key value only for the signal intensity μ_S .

This SDP is infinite dimensional, and so following Eq. (49) from Ref. [28] we use the dimension reduction method. This technique involves taking a projection Π_N onto the subspace containing less than $N + 1$ photons, to construct a finite-dimensional SDP that would lower bound the infinite-dimensional SDP. The finite-dimensional SDP is given as

$$\begin{aligned}
 R^N &= \min_{\rho_{AA_S B}^N} f(\rho_{AA_S B}^N) - \delta_{\text{leak}} \\
 &\text{s.t. } \gamma_{j|i, \mu} - W^\mu \leq \text{Tr}[\Gamma_j^N \Phi(\rho_i^\mu)] \\
 &\leq \gamma_{j|i, \mu} \quad \forall i, j, \mu \\
 1 - W &\leq \text{Tr}[\rho_{AA_S B}^N] \leq 1 \\
 \text{Tr}_B[\rho_{AA_S B}^N] &\leq \rho_{AA_S},
 \end{aligned} \quad (3)$$

where $\rho_{AA_S B}^N = (\mathbb{I}_{AA_S} \otimes \Pi_N) \rho_{AA_S B} (\mathbb{I}_{AA_S} \otimes \Pi_N)$ and $\Gamma_j^N = \Pi_N \Gamma_j \Pi_N$. W is a parameter that needs to be estimated from Bob's observations that signifies the weight of $\rho_{AA_S B}$ that lies outside the subspace we are projecting on, i.e., $W \geq 1 - \text{Tr}[\rho_{AA_S B}^N]$. Note that we have used $[\Gamma_j, \Pi_N] = 0$ to obtain tighter constraints. This condition is commonly satisfied when we talk about photon-counting receiver modules that are block diagonal in the total photon number. However, it is not crucial to use this and more details on obtaining the key rate for the fully general case are given in Ref. [28].

The SDP can be further simplified if the signal states have some block-diagonal structure and can be written as a direct sum $\rho_i^{\mu_S} = \bigoplus_{\tilde{n}=0}^{\infty} p_{\tilde{n}} \rho_i^{\tilde{n}}$ where the block-diagonal structure is the same for all the signals i . Here, μ_S denotes the signal intensity. This is obviously the case when we use fully phase-randomized states where $|\tilde{n}\rangle$ directly represents the photon number. As we shall show in Sec. IV D, we can obtain similar structure with partially phase-randomized states as well.

Following Eqs. (D.6) and (D.9) from Ref. [29], we can exploit the block-diagonal structure to write $f(\rho_{AA_S B}) = \sum_{\tilde{n}=0}^{\infty} p_{\tilde{n}} f(\rho_{AB}^{\tilde{n}})$ as a sum of positive terms. Thus, taking finitely many of these terms is sufficient to lower bound the key rate. In practice, just one of these terms is usually enough to give a good bound on the key rate for most protocols. For example, in a standard decoy-state protocol with fully phase-randomized states, considering just the term corresponding to single photons is sufficient to give a useful lower bound on the key rate.

If we could find the statistics to constrain each of these terms as $Y_{\tilde{n}}^L(i, j) \leq \text{Tr}[\Gamma_j^N \Phi(\rho_i^{\tilde{n}})] \leq Y_{\tilde{n}}^U(i, j)$, we could obtain the set of SDPs

$$\begin{aligned}
 R_{\tilde{n}}^N &= \min_{\rho_{AB}^{\tilde{n}N}} p_{\tilde{n}} f(\rho_{AB}^{\tilde{n}N}) \\
 &\text{such that } Y_{\tilde{n}}^L(i, j) \leq \text{Tr}[\Gamma_j^N \Phi(\rho_i^{\tilde{n}})] \leq Y_{\tilde{n}}^U(i, j) \\
 \text{Tr}_B[\rho_{AB}^{\tilde{n}N}] &\leq \rho_A^{\tilde{n}} \\
 1 - W_{\tilde{n}} &\leq \text{Tr}[\rho_{AB}^{\tilde{n}N}] \leq 1 \\
 \rho_{AB}^{\tilde{n}N} &\geq 0,
 \end{aligned} \quad (4)$$

which can be related to the key rate as $R^N = \sum_{\tilde{n}} R_{\tilde{n}}^N - \delta_{\text{leak}}$. Note that solving each of these SDPs independently will introduce some looseness since we do not take into account the fact that the constraints of different blocks are in general correlated. We describe improved methods to upper and lower bound $\text{Tr} \left[\Gamma_j^N \Phi(\rho_i^{\tilde{n}}) \right]$ via the generalized decoy-state analysis described in Sec. IV.

To summarize, if we have an IID protocol, signal states that are all block diagonal in the same basis, and we have bounds on the statistics of each signal state block, then the set of SDPs described in Eq. (4) help us reliably lower bound the key rate of the protocol.

C. Source maps

We will now describe a commonly used class of source-replacement schemes, which we call source maps, with ideas similar to squashing maps [30]. In general, source maps simplify security proofs at the cost of loosening our key-rate bounds and giving Eve more power than she has in reality.

Definition 1 (Source map).—Let $\{\rho_i\} \in \mathcal{D}(\mathcal{H})$ and $\{\tau_i\} \in \mathcal{D}(\mathcal{K})$ be the set of states Alice prepares for two QKD protocols where the rest of the protocol is the same. A channel Ψ from $\mathcal{D}(\mathcal{K})$ to $\mathcal{D}(\mathcal{H})$ is a **source map** if $\rho_i = \Psi(\tau_i)$ for all i . We call the protocol where Alice produces the states $\{\rho_i\}$ ($\{\tau_i\}$) a real (virtual) protocol with real (virtual) states.

Let R_ρ^∞ and R_τ^∞ be the asymptotic key rates for identical observations $\gamma_{j|i}$ of the real and virtual QKD protocols, respectively. The key rates are related as $R_\tau^\infty \leq R_\rho^\infty$. Intuitively, this can be seen from Fig. 1 where giving Eve the source map gives her more power. A more formal proof of this fact is given in Appendix A 1.

Note that in the above definition, the different signal states $\{\rho_i\}$ and $\{\tau_i\}$ that Alice prepares could represent the joint state sent for multiple key generation rounds of the protocol. Thus, this does not assume either IID signal states or IID attacks by Eve, and is completely general.

As an example of a source map that we shall use, we describe virtual states call block-tagged states [31]. Consider a protocol with an IID source that produces real states $\rho_i^{\mu S} = V_i \rho^{\mu S} V_i^\dagger$ where $\rho^{\mu S}$ can be diagonalized as $\rho^{\mu S} = \sum_{\tilde{n}} p_{\tilde{n}} |\tilde{n}\rangle \langle \tilde{n}|$. We can then define the virtual “block-tagged” states as $\tau_i = \sum_{\tilde{n}} p_{\tilde{n}} V_i (|\tilde{n}\rangle \langle \tilde{n}|) V_i^\dagger \otimes |\tilde{n}\rangle \langle \tilde{n}|$, and the source map $\Psi = \mathbb{I} \otimes \text{Tr}$ that reproduces the real states from the virtual states is the partial trace over the second system. We call this simplification block tagging.

The block-diagonal structure of the block-tagged states simplifies the objective function by breaking it up into individual blocks [22] as $f(\rho^N) = \sum_{\tilde{n}} p_{\tilde{n}} f(\rho_{\tilde{n}}^N)$ where

$$\rho_{\tilde{n}}^N = \sum_{ij} \sqrt{p(i)p(j)} |i\rangle \langle j|_A \otimes \Pi_N \Phi \left(V_i (|\tilde{n}\rangle \langle \tilde{n}|) V_j^\dagger \otimes |\tilde{n}\rangle \langle \tilde{n}| \right)_B \Pi_N.$$

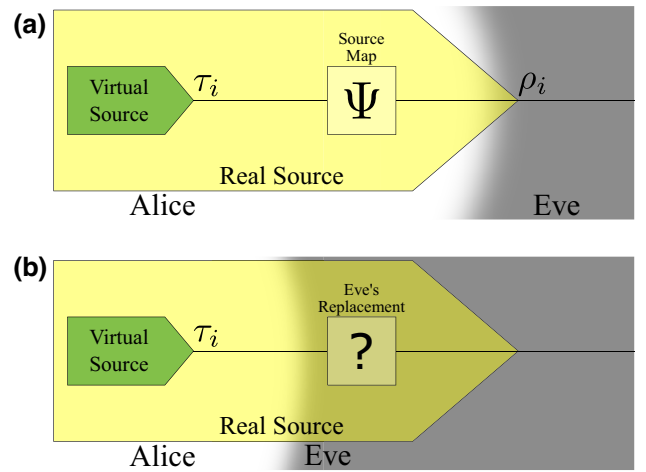


FIG. 1. The real source can always be replaced by the virtual source in security proofs if they are related via a source map since the virtual source gives Eve more power. (a) We can model the real source as a virtual source followed by a source map since they both have the exact same output and (b) once we give Eve control of the source map, she can perform any physical operation on the output of the virtual source, including the source map Ψ if reproducing the real state is optimal for her.

Thus, we can use Eq. (4) to bound the key rate even if the real states do not have the block-diagonal structure. This simplification comes at the cost of key rate in the case that the isometries do not retain the block-diagonal structure of the state, i.e., $\langle \tilde{n} | V_i^\dagger V_j | \tilde{m} \rangle \neq 0$ for some $\tilde{n} \neq \tilde{m}$. We note that a key rate simplification similar to Eq. (4) was first seen in the context of discrete-phase-randomized decoy-state QKD in Ref. [32], although they use different techniques to arrive at the result.

III. PHASE IMPERFECTIONS IN QKD

We shall first discuss a simplified model of phase imperfections that we consider. We then describe a source map that connects a model IID state to the imperfect state for a large class of QKD protocols. Finally, we also discuss some of the difficulties in characterizing the relevant parameters to construct the model IID state from the actual laser state.

We model a sequence of laser pulses as a probabilistic mixture of coherent states, where different laser pulses are independent of each other. Since we consider only phase imperfections, we assume that the intensity of each laser pulse is the same. Such a state can be the result of an active laser-seeding attack [16] as discussed in Ref. [15]. Under these assumptions, the general state for the sequence of

laser pulses can be written as

$$\rho_{\text{laser}}^{\mu} = \int d\phi_1 \dots d\phi_n p_{\Phi_1}(\phi_1) \dots p_{\Phi_n}(\phi_n) \times |\sqrt{\mu}e^{i\phi_1}\rangle\langle\sqrt{\mu}e^{i\phi_1}| \otimes \dots \otimes |\sqrt{\mu}e^{i\phi_n}\rangle\langle\sqrt{\mu}e^{i\phi_n}|. \quad (5)$$

We will show that we can replace this general source state by a simplified state that is IID and is of the form

$$(\rho_{\text{model}}^{\mu})^{\otimes n} = \left(q \int d\phi \frac{1}{(2\pi)^n} |\sqrt{\mu}e^{i\phi}\rangle\langle\sqrt{\mu}e^{i\phi}| + (1-q) |\sqrt{\mu}\rangle\langle\sqrt{\mu}| \right)^{\otimes n}, \quad (6)$$

where $q := \min_k \min_{\phi_k} 2\pi p_{\Phi_k}(\phi_k)$ is a parameter that must be characterized, which represents the degree to which the sequence of laser pulses are phase randomized. Although characterizing this parameter might pose some practical difficulties, it is still significantly easier than characterizing each probability density function p_{Φ_k} .

A. Source map for non-IID laser

We now explicitly construct a physical map that connects the model laser state to the actual laser state with phase distribution $p_{\Phi_1 \dots \Phi_n}(\phi_1 \dots \phi_n) = p_{\Phi_1}(\phi_1) \dots p_{\Phi_n}(\phi_n)$ with associated parameter q as shown in Fig. 2. As a first step toward the source map construction, we consider the action of a phase modulator on the model laser state. The phase modulator modulates the phase of the i th pulse with probability $(p_{\Phi_i}(\phi_i) - q/2\pi)/1 - q$ for all i . The model laser source together with this phase modulator will imitate the actual laser source i.e., $\rho_{\text{laser}}^{\mu} = \Phi(\rho_{\text{model}}^{\mu})$ where Φ represents the action of the phase modulator as described above. We give a proof of this in Appendix A 2.

However the definition of the source map Ψ requires that $\Xi_i^{\otimes n}(\rho_{\text{laser}}^{\mu}) = \Psi(\Xi_i(\rho_{\text{model}}^{\mu})^{\otimes n})$ for all signal states i where Ξ_i denotes the preparation channel that acts on a

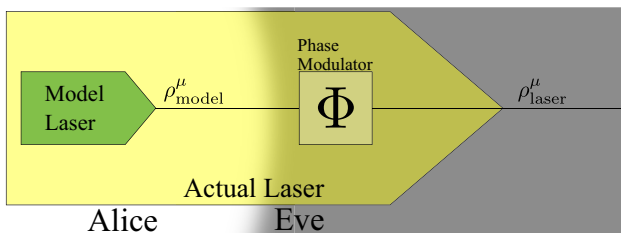


FIG. 2. Replace the actual laser source with a model laser source and a phase modulator. We can then give the phase modulator to Eve. This would increase the power that Eve has and thus the key rate using the model laser source would lower bound the key rate using the actual laser source.

single pulse to prepare the final signal state for a single round of the protocol. We can construct the source map Ψ for a large class of QKD protocols analogously to how we constructed the map Φ . Intuitively, this construction holds when the preparation channels Ξ_i for the protocol “commute” with the action of the phase modulator Φ .

For example, consider a QKD protocol that uses time-bin encoding Ξ_i where a single laser pulse is split into a block of two pulses with possible phase coherences across pulses. We construct the source map Ψ through the action of a phase modulator that modulates the phase of the laser pulses as follows: the i th block of pulses (which all are the output of the action of Ξ_i on the i th laser pulse from $\rho_{\text{model}}^{\mu}$) are all modulated with the same phase ϕ_i with probability $(p_{\Phi_i}(\phi_i) - q/2\pi)/1 - q$ for all i . Note that this source map can be naturally extended to blocks with more than two pulses.

The source map we constructed would commute with any intensity modulation of the laser pulse. So, this would also be a valid source map for decoy-state protocols. Thus, the key rate of the virtual protocol with an IID characterized laser source and preparation channels Ξ_i would lower bound the key rate of the real protocol with the partially characterized nonidentically distributed laser source and preparation channels Ξ_i .

B. Experimental characterization of laser

We have constructed a source map from an uncorrelated laser source with different probability density functions p_{Φ_i} for each pulse, all satisfying $p_{\Phi_i}(\phi_i) \geq q/2\pi \forall i, \phi_i$. Thus, the experimental problem has been reduced from characterizing the probability density function for each pulse, to characterizing a single parameter q that represents the degree of phase randomization. Although this problem is a significantly simpler problem to solve, standard visibility measurements do not directly measure this quantity.

The visibility experiment as described in Sec. II. A. of Ref. [14], is performed with a train consecutive laser pulses passed through an interferometer with a phase shifter in one arm. We have illustrated this with two pulses in Fig. 3. The intensity of the light arriving at the middle time slot of the detector is measured for different values of the phase shift θ . We assume that the pulses have the same intensity.

The phase difference θ between the paths is varied to calculate the visibility V given by

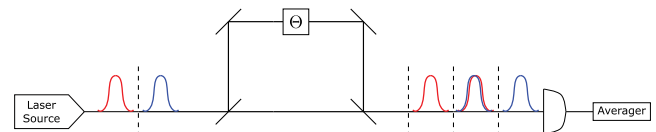


FIG. 3. Schematic illustration of the experimental setup described in Ref. [14]. The phase difference θ between the paths can be modulated with the phase shifter Θ .

$$V = \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}}, \quad (7)$$

$$= \frac{\langle \cos(\theta + \phi) \rangle_{\max} - \langle \cos(\theta + \phi) \rangle_{\min}}{2 + \langle \cos(\theta + \phi) \rangle_{\max} + \langle \cos(\theta + \phi) \rangle_{\min}}, \quad (8)$$

where the maximum and minimum is over all θ , and ϕ is the difference in the phase of the adjacent pulses.

Note that the measurement as described in Ref. [14] is used to measure phase correlations between adjacent pulses. However, due to limitations in our security proof techniques, we assume that the pulses are independent of each other. Moreover, the visibility measurement does not directly measure the degree of phase randomization q directly as visibility measures other effects like the temporal distribution of the laser pulses. Thus, using this experiment to obtain the extent of phase randomization q requires us to make further model assumptions for the probability distribution.

As an illustrative example consider two different model assumptions for the phase distribution:

(i) The phase distribution is the same as in the model laser state, i.e., $p_{\Phi_i}(\phi_i) = (q/2\pi) + (1 - q)\delta(\phi_i)$. We can then calculate

$$q = 1 - \sqrt{V}. \quad (9)$$

(ii) The phase distribution of each pulse is a wrapped normal distribution with standard deviation σ centered about the origin, i.e., $p_{\Phi_i}(\phi_i) = 1/\sqrt{2\pi\sigma^2} \sum_{k=-\infty}^{\infty} \exp[-(\phi_i + 2\pi k)^2/2\sigma^2]$. We can relate the visibility to the standard deviation as

$$V = \exp[-\sigma^2]. \quad (10)$$

As this completely characterizes the wrapped normal distribution, we can use this to numerically find the extent of phase randomization q .

These values of q computed under different model assumptions are, in general, different. Thus, it would be interesting to develop other techniques that more directly measures this quantity and reduces the number of assumptions that we need to make.

To summarize, we have made two model assumptions on the laser state.

(1) The first model assumption is a limitation of our security proof techniques and can be stated as follows. The laser outputs a

- (a) probabilistic mixture of coherent states
- (b) same intensity, and
- (c) independent phase distribution.

Thus, the state can be written as

$$\rho_{\text{laser}}^{\mu} = \int d\phi_1 \dots d\phi_n p_{\Phi_1}(\phi_1) \dots p_{\Phi_n}(\phi_n) \times |\sqrt{\mu}e^{i\phi_1}\rangle\langle\sqrt{\mu}e^{i\phi_1}| \otimes \dots \otimes |\sqrt{\mu}e^{i\phi_n}\rangle\langle\sqrt{\mu}e^{i\phi_n}|.$$

Assumption B has been lifted in Ref. [15].

(2) The second assumption is due to limitations in the current experiments used to quantify the degree of phase randomization q . These further model assumptions on $p_{\Phi_i}(\phi_i)$ might be physically motivated. For example,

(a) $p_{\Phi_i}(\phi_i) = (q/2\pi) + (1 - q)\delta(\phi_i)$,

(b) $p_{\Phi_i}(\phi_i)$ is a wrapped normal distribution centered about the origin with standard deviation σ .

Thus, it would be of practical interest to design other experiments to bound the minimum of the phase distribution without making such model assumptions.

IV. GENERALIZED DECOY-STATE ANALYSIS

The standard decoy-state analysis relies on the assumption that the laser pulses are completely phase randomized, hence block diagonal. Additionally, it requires that the weight of each block is independent of the encoding used. However, the methods described in Sec. III result in partially phase-randomised states of the form shown in Eq. (6). We first formulate the decoy-state problem abstractly by drawing an analogy to channel tomography in Sec. IV A.

For an IID fully phase-randomized source, we show in Sec. IV B how the general formulation simplifies to the standard decoy-state analysis [10,11]. We stress the relevance of the generalized decoy-state analysis for nonideal sources as seen in Sec. III since the standard decoy-state analysis cannot be used for laser states of the form described by Eq. (6).

The general framework of our generalized decoy-state analysis typically takes the form of infinite-dimensional SDPs. In Sec. IV C, we introduce finite projections to construct a related finite-dimensional SDP that facilitates numerical evaluation. Finally, in Sec. IV D we describe a useful loosening of the SDP to reduce the dimensions while using it for typical QKD protocols.

A. General framework

First, to set up notation, let $\rho_{\mu}^k, \sigma_i \in \mathcal{D}(\mathcal{H})$ be density operators on \mathcal{H} , which we shall call the state space. Let $\Gamma_l, F_j \in \text{Pos}(\mathcal{K})$ be POVM elements on \mathcal{K} , which we shall call the measurement space. Let $\Phi : \mathcal{L}(\mathcal{H}) \rightarrow \mathcal{L}(\mathcal{K})$ be a quantum channel.

We are given the statistics $\{\gamma_{l|k,\mu}\}$ of the input states $\{\rho_k^{\mu}\}$ to the unknown channel Φ where the output is measured by the POVM elements $\{\Gamma_l\}$ as $\text{Tr}[\Gamma_l \Phi(\rho_k^{\mu})] = \gamma_{l|k,\mu}$. We call these the actual states and POVM elements, respectively. From this we seek to bound the statistics for

a possibly different set of input states $\{\sigma_i\}$ and POVM elements $\{F_j\}$ measuring the output of the same channel Φ , which can be written as $\text{Tr}[F_j \Phi(\sigma_i)]$. We call these virtual states and POVM elements, and define a matrix Y whose elements are the statistics $Y(i, j) = \text{Tr}[F_j \Phi(\sigma_i)]$.

More formally, we are interested in the set \mathbb{Y} of all matrices Y with elements $Y(i, j) = \text{Tr}[\Phi(\sigma_i)F_j]$ with constraints on Φ given by

$$\begin{aligned} \text{Tr}[\Phi(\rho_k^\mu)\Gamma_l] &= \gamma_{l|k,\mu} \quad \forall k, l, \mu \\ \Phi &\text{ is CPTP.} \end{aligned} \quad (11)$$

Note that here the different elements $Y(i, j)$ are not independent of each other for $Y \in \mathbb{Y}$. This makes it hard to find and use \mathbb{Y} . Thus, to make it easier to use, we define $Y^L(i, j) = \inf_{Y \in \mathbb{Y}} Y(i, j)$, and $Y^U(i, j) = \sup_{Y \in \mathbb{Y}} Y(i, j)$. These can now be independently written as the solution to the set of optimisation problems as follows:

$$\begin{aligned} Y^L(i, j) &= \min_{\Phi} \text{Tr}[\Phi(\sigma_i)F_j] \\ \text{s.t. } \text{Tr}[\Phi(\rho_k^\mu)\Gamma_l] &= \gamma_{l|k,\mu} \quad \forall k, l, \mu \\ \Phi &\text{ is CPTP.} \end{aligned} \quad (12)$$

$$\begin{aligned} Y^U(i, j) &= \max_{\Phi} \text{Tr}[\Phi(\sigma_i)F_j] \\ \text{s.t. } \text{Tr}[\Phi(\rho_k^\mu)\Gamma_l] &= \gamma_{l|k,\mu} \quad \forall k, l, \mu \\ \Phi &\text{ is CPTP.} \end{aligned} \quad (13)$$

This simplification is a relaxation of our initial problem to independent optimisations for each virtual state i and outcome j . As a result of this relaxation, we might sometimes see counterintuitive behavior as illustrated by the following example. In the absence of this relaxation, we know that computing bounds for the sum of virtual POVM elements would be the same as computing and then summing the individual bounds. However, counterintuitively solving these relaxed SDPs for sums of virtual POVM elements might lead to better bounds than solving and then summing the optimal values of the individual SDPs. This is not a fundamental limitation as it does not affect the original optimization. It is a direct consequence of the relaxation we have made to bound these statistics.

The optimization problems described in Eqs. (11) and (12) can be reframed as SDPs by considering the Choi-Jamiolkowski isomorphism of the channel J

$$\begin{aligned} \text{opt. } \text{Tr}_J [(\sigma_i^T \otimes F_j)J] \\ \text{s.t. } \text{Tr}[(\rho_k^{\mu T} \otimes \Gamma_l)J] &= \gamma_{l|k,\mu} \quad \forall k, l, \mu, \\ J &\geq 0 \\ \text{Tr}_{\mathcal{K}}[J] &= \mathbb{I}_{\mathcal{H}} \end{aligned} \quad (14)$$

where opt. indicates that we have to optimize the objective function to find both the maximum and the minimum as separate SDPs. In order to simplify notation, let S_∞ be the feasible set of the SDP, i.e.,

$$\begin{aligned} S_\infty := \left\{ J \in \mathcal{B}(\mathcal{H} \otimes \mathcal{K}) \mid \text{Tr}_{\mathcal{K}}[J] = \mathbb{I}_{\mathcal{H}}, J \geq 0, \right. \\ \left. \text{Tr}[(\rho_k^{\mu T} \otimes \Gamma_l)J] = \gamma_{l|k,\mu} \quad \forall k, l, \mu \right\}. \end{aligned} \quad (15)$$

B. Standard decoy

In the special case where the laser emits states ρ_{PR}^μ that are fully phase-randomized states with intensity μ , we show how our general analysis given in Eq. (14) reduces to the standard decoy-state analysis.

The actual states $\{\rho_k^\mu\}$ are obtained by the action of the preparation channels $\{\Xi_k\}$ on the fully phase-randomized laser state as $\rho_k^\mu = \Xi_k(\rho_{\text{PR}}^\mu)$. The virtual states that we can use in Eq. (14) are the n -photon states for different encodings, i.e., $\sigma_i^n = \Xi_i(|n\rangle\langle n|)$. The crucial assumption here is that each of the actual states can be written as a classical mixture of the virtual states as

$$\begin{aligned} \rho_i^\mu &= \sum_n p_\mu(n) \Xi(|n\rangle\langle n|) \\ &= \sum_n p_\mu(n) \sigma_i^n. \end{aligned} \quad (16)$$

The actual POVM elements Γ_j are obtained from the measurement setup. The virtual POVM elements whose outcomes we bound are the same as the actual POVM elements $F_j = \Gamma_j$.

With these definitions, we can rewrite the SDPs in Eq. (14) as

$$\begin{aligned} \text{opt. } \text{Tr}_J [(\Xi_i(|n\rangle\langle n|)^T \otimes \Gamma_j)J] \\ \text{such that } \text{Tr}[(\rho_k^{\mu T} \otimes \Gamma_l)J] &= \gamma_{l|k,\mu} \quad \forall k, l, \mu \\ J &\geq 0 \\ \text{Tr}_{\mathcal{K}}[J] &= \mathbb{I}_{\mathcal{H}}. \end{aligned} \quad (17)$$

The constraints in this case simplify as follows:

$$\begin{aligned} \text{Tr}[(\rho_k^{\mu T} \otimes \Gamma_l)J] &= \text{Tr}[\Phi(\rho_k^\mu)\Gamma_l] \\ &= \text{Tr}\left[\Phi\left(\sum_n p_\mu(n) \Xi_k(|n\rangle\langle n|)\right)\Gamma_l\right] \end{aligned} \quad (18)$$

$$= \sum_n p_\mu(n) \text{Tr}[\Phi(\Xi_k(|n\rangle\langle n|))\Gamma_l] \quad (19)$$

$$= \sum_n p_\mu(n) p(l|k, n) = \gamma_{l|k,\mu}, \quad (20)$$

$$= \sum_n p_\mu(n) p(l|k, n) = \gamma_{l|k,\mu}, \quad (21)$$

First, we set up some notation. Given a projection Π_M , we can define the off-diagonal blocks $H_k^\mu := \rho_k^\mu - \rho_k^{\mu M} - \rho_k^{\mu \bar{M}}$ where $\rho_k^{\mu M} := \Pi_M \rho_k^\mu \Pi_M$, and $\rho_k^{\mu \bar{M}} := \bar{\Pi}_M \rho_k^\mu \bar{\Pi}_M$. We also define the weight $w_{kM}^\mu := \text{Tr}[\rho_k^{\mu \bar{M}}]$ of the k th input state outside the Π_M projected subspace. This can be further used to define $\epsilon_{kM}^\mu := \lambda_{kM}^\mu \sqrt{w_{kM}^\mu}$, which measures how “big” the off-diagonal block is where $\lambda_{kM}^\mu := \left\| \sqrt{\rho_k^{\mu M}} \Pi_M \rho_k^\mu \bar{\Pi}_M \sqrt{\rho_k^{\mu \bar{M}}} \right\|_\infty$ and A^g is the generalized inverse of A . These definitions are used in the following lemma whose proof can be found in Appendix B 3.

Lemma 2.—Define

$$\begin{aligned} E_M &:= \{J^M \in \mathcal{B}(\mathcal{H}_M \otimes \mathcal{K}) \mid \text{Tr}_{\mathcal{K}}[J^M] \leq \Pi_M, \\ &J^M \geq 0, \text{Tr}[(\rho_k^{\mu T} \otimes \Gamma_l)J^M] \leq \gamma_{l|k,\mu} + \epsilon_{kM}^\mu, \\ &\text{Tr}[(\rho_k^{\mu T} \otimes \Gamma_l)J^M] \geq \gamma_{l|k,\mu} - w_{kM}^\mu - \epsilon_{kM}^\mu \forall k, l, \mu\}. \end{aligned} \quad (26)$$

Then, $(\Pi_M \otimes \mathbb{I}_{\mathcal{K}}) S_\infty (\Pi_M \otimes \mathbb{I}_{\mathcal{K}}) \subseteq E_M$ where S_∞ is as defined in Eq. (15).

The last step to construct the set S_{MN} requires that we estimate an additional quantity. We need to find bounds on the weight W_{kN}^μ of the transmitted state $\Phi(\rho_k^\mu)$ outside the Π_N projected subspace defined as $\text{Tr}[\Phi(\rho_k^\mu)\Pi_N] \geq 1 - W_{kN}^\mu$. Equivalently, this can be written as

$$\text{Tr}[(\rho_k^{\mu T} \otimes \Pi_N)J] \geq 1 - W_{kN}^\mu, \quad (27)$$

where $J \in S_\infty$. The method to find this bound is protocol dependent, and can be derived from the expectation value constraints on $J \in S_\infty$. As an example, we have described one such method to find the bound for the three-state protocol in Appendix C.

This leads us to the explicit construction of S_{MN} when the POVM elements Γ_l commute with the projection Π_N .

Lemma 3.—Let $[\Pi_N, \Gamma_l] = 0 \forall l$, and define

$$\begin{aligned} S_{MN} &:= \{J^{MN} \in \mathcal{B}(\mathcal{H}_M \otimes \mathcal{K}_{N'}) \mid \\ &\text{Tr}_{\mathcal{K}}[J^{MN}] \leq \Pi_M, J^{MN} \geq 0, \\ &\text{Tr}[(\rho_k^{\mu T} \otimes \Gamma_l)J^{MN}] \geq \gamma_{l|k,\mu} - W_{kN}^\mu - w_{kM}^\mu - 2\epsilon_{kM}^\mu, \\ &\text{Tr}[(\rho_k^{\mu T} \otimes \Gamma_l)J^{MN}] \leq \gamma_{l|k,\mu} + \epsilon_{kM}^\mu \forall k, l, \mu\}. \end{aligned} \quad (28)$$

Then, $(\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) E_M (\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) \subseteq S_{MN}$ where E_M is as defined in Eq. (26).

The proof of the above lemma can be found in Appendix B 4. The following corollary is a direct consequence of Lemma 2 and Lemma 3.

Corollary 3.1.— $(\Pi_M \otimes \Pi_N) S_\infty (\Pi_M \otimes \Pi_N) \subseteq S_{MN}$.

Proof.—

$$\begin{aligned} &(\Pi_M \otimes \Pi_N) S_\infty (\Pi_M \otimes \Pi_N) \\ &= (\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) ((\Pi_M \otimes \mathbb{I}_{\mathcal{K}}) S_\infty (\Pi_M \otimes \mathbb{I}_{\mathcal{K}})) (\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) \\ &\subseteq (\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) E_M (\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) \\ &\subseteq S_{MN}, \end{aligned}$$

where the first inclusion follows from Lemma 2, and the second follows from Lemma 3. \blacksquare

3. Objective function

Having constructed S_{MN} , we now relate the objective function $\text{Tr}[(\sigma_i^T \otimes F_j)J^{MN}]$ to $Y(i, j) = \text{Tr}[(\sigma_i^T \otimes F_j)J]$ where $J^{MN} \in S_{MN}$ and $J \in S_\infty$. This subsection thus completes the construction of the finite-dimensional SDP and relates it to the infinite-dimensional SDP of interest as outlined at the start of Sec. IV C.

We first define $w_{iM} := \text{Tr}[\sigma_i^{\bar{M}}]$, and $\lambda_{iM} := \left\| \sqrt{\sigma_i^{\bar{M}}} \Pi_M \sigma_i \bar{\Pi}_M \sqrt{\sigma_i^{\bar{M}}} \right\|_\infty$ similar to the definitions at the start of Sec. IV C 2. Recall also that we defined $Y^U(i, j) = \max_{J \in S_\infty} \text{Tr}[(\sigma_i^T \otimes F_j)J]$ and $Y^L(i, j) = \min_{J \in S_\infty} \text{Tr}[(\sigma_i^T \otimes F_j)J]$.

First, we consider virtual POVM elements $F \in \mathcal{B}(\mathcal{K}_N)$ that live in the finite-dimensional subspace described by Π_N . This is indeed the case of interest for the key-rate SDP described in Eq. (4).

Theorem 4.—Let $F_j \in \mathcal{B}(\mathcal{K}_N)$ be POVM elements such that $F_j = \Pi_N F_j \Pi_N$. Then

$$Y^L(i, j) \geq \min_{J^{MN} \in S_{MN}} \text{Tr}[(\sigma_i^T \otimes F_j)J^{MN}] - \epsilon_{iM}, \quad (29)$$

$$Y^U(i, j) \leq \max_{J^{MN} \in S_{MN}} \text{Tr}[(\sigma_i^T \otimes F_j)J^{MN}] + w_{iM} + \epsilon_{iM}, \quad (30)$$

where $\epsilon_{iM} := \lambda_{iM} \sqrt{w_{iM}}$.

Proof.—Let J^U and J^L be the optimal operators in S_∞ such that

$$Y^U(i, j) = \text{Tr}[(\sigma_i^T \otimes F_j)J^U], \quad (31)$$

$$Y^L(i, j) = \text{Tr}[(\sigma_i^T \otimes F_j)J^L]. \quad (32)$$

Noting that $\Pi_N F_j \Pi_N = F_j$, we infer from Lemma 2 that

$$\begin{aligned} Y^L(i, j) &\geq \text{Tr}[(\sigma_i^T \otimes F_j) (\Pi_M \otimes \Pi_N) J^L (\Pi_M \otimes \Pi_N)] \\ &\quad - \epsilon_{iM}, \end{aligned} \quad (33)$$

$$\begin{aligned} Y^U(i, j) &\leq \text{Tr}[(\sigma_i^T \otimes F_j) (\Pi_M \otimes \Pi_N) J^U (\Pi_M \otimes \Pi_N)] \\ &\quad + w_{iM} + \epsilon_{iM}. \end{aligned} \quad (34)$$

Corollary 3.1 implies that $(\Pi_M \otimes \Pi_N)J^L(\Pi_M \otimes \Pi_N) \in S_{MN}$, and $(\Pi_M \otimes \Pi_N)J^U(\Pi_M \otimes \Pi_N) \in S_{MN}$. Thus we get

$$\begin{aligned} & \min_{J^{MN} \in S_{MN}} \text{Tr}[(\sigma_i^T \otimes F_j)J^{MN}] \\ & \leq \text{Tr}[(\sigma_i^T \otimes F_j)(\Pi_M \otimes \Pi_N)J^L(\Pi_M \otimes \Pi_N)], \quad (35) \\ & \max_{J^{MN} \in S_{MN}} \text{Tr}[(\sigma_i^T \otimes F_j)J^{MN}] \\ & \geq \text{Tr}[(\sigma_i^T \otimes F_j)(\Pi_M \otimes \Pi_N)J^U(\Pi_M \otimes \Pi_N)]. \quad (36) \end{aligned}$$

Chaining these inequalities completes the proof. \blacksquare

Next, we consider the more general case where the POVM elements do not live in a finite-dimensional subspace. We first use Theorem 4 to find the bound $\text{Tr}[(\sigma_i^T \otimes \Pi_N)J] \geq 1 - W_{iN}$ by choosing $F_j = \Pi_N$ and numerically solving the finite-dimensional SDP $\min_{J^{MN} \in S_{MN}} \text{Tr}[(\sigma_i^T \otimes \Pi_N)J^{MN}]$. This can be used to state the following, more general theorem.

Theorem 5.—Let $F_j \in \mathcal{B}(\mathcal{K})$ be a POVM element such that $F_j = F_j^N + F_j^{\bar{N}}$. Then

$$Y^L(i, j) \geq \min_{J^{MN} \in S_{MN}} \text{Tr}[(\sigma_i^T \otimes F_j)J^{MN}] - \epsilon_{iM}, \quad (37)$$

$$\begin{aligned} Y^U(i, j) & \leq \max_{J^{MN} \in S_{MN}} \text{Tr}[(\sigma_i^T \otimes F_j)J^{MN}] + W_{iN} \\ & \quad + w_{iM} + 2\epsilon_{iM}. \quad (38) \end{aligned}$$

Proof.—Similar to the proof of Theorem 4, pick J^U and J^L as the optimal operators in S_∞ such that

$$Y^U(i, j) = \text{Tr}[(\sigma_i^T \otimes F_j)J^U], \quad (39)$$

$$Y^L(i, j) = \text{Tr}[(\sigma_i^T \otimes F_j)J^L]. \quad (40)$$

From Lemma 3, we can show that

$$\begin{aligned} Y^L(i, j) & \geq \text{Tr}[(\sigma_i^T \otimes F_j)(\Pi_M \otimes \Pi_N)J^L(\Pi_M \otimes \Pi_N)] \\ & \quad - \epsilon_{iM}, \quad (41) \end{aligned}$$

$$\begin{aligned} Y^U(i, j) & \leq \text{Tr}[(\sigma_i^T \otimes F_j)(\Pi_M \otimes \Pi_N)J^U(\Pi_M \otimes \Pi_N)] \\ & \quad + W_{iN} + w_{iM} + 2\epsilon_{iM}. \quad (42) \end{aligned}$$

The rest of the proof uses Corollary 3.1 and is identical to the proof of Theorem 4. \blacksquare

Theorems 4 and 5 let us bound $Y(i, j)$ in terms of the solution to a finite-dimensional SDP. This can be done numerically. We note here that this generalized decoy-state analysis is fairly general and can also be applied outside decoy-state QKD, for example, to bound the statistics of cat states in Ref. [34] by sending fully phase-randomized states.

D. Application to decoy-state QKD

We shall now detail how we can apply these methods to a general decoy-state QKD protocol. We also detail a protocol-dependent relaxation that reduces dimensions for more efficient computation. To this end, consider a QKD protocol with signal states $\rho_i^{\mu S}$ that are compatible with isometric preparation channels Ξ_i as $\rho_i^{\mu S} = \Xi_i(\rho^{\mu S})$. Assume that the base state $\rho^{\mu S}$ can be diagonalized as

$$\rho^{\mu S} = \sum_{\tilde{n}} p_{\tilde{n}} |\tilde{n}\rangle\langle\tilde{n}|. \quad (43)$$

We can block tag these signal states with the eigenvectors $|\tilde{n}\rangle$ as described in Sec. II C. Our key-rate optimization then reduces to the SDP given in Eq. (4). As shown in Eq. (4), we need to compute upper ($Y_{\tilde{n}}^U(i, j)$) and lower ($Y_{\tilde{n}}^L(i, j)$) bounds on $\text{Tr}[\Gamma_j^N \Phi(|\tilde{n}\rangle\langle\tilde{n}|)]$. This can be done directly by using the generalized decoy-state analysis described above. We choose the virtual states $\sigma_{i, \tilde{n}} = \Xi_i(|\tilde{n}\rangle\langle\tilde{n}|)$, actual states $\{\rho_i^\mu\}$, actual POVM elements $\{\Gamma_j\}$, and virtual POVM elements $\{\Gamma_j^N\}$ for the analysis. The set of finite-dimensional SDPs resulting from the generalized decoy-state analysis can be written as

$$\begin{aligned} & \text{opt.}_{J^{MN}} \text{Tr}[(\sigma_{i, \tilde{n}}^{MT} \otimes F_j^N)J^{MN}] \\ & \text{such that } \text{Tr}[(\rho_k^{\mu MT} \otimes \Gamma_l^N)J^{MN}] \leq \gamma_{|k, \mu} + \epsilon_{kM}^\mu \\ & \quad \text{Tr}[(\rho_k^{\mu MT} \otimes \Gamma_l^N)J^{MN}] \geq \gamma_{|k, \mu} - W_{kN}^\mu - w_{kM}^\mu \\ & \quad \quad - 2\epsilon_{kM}^\mu \quad \forall k, l, \mu \\ & J^{MN} \geq 0 \\ & \text{Tr}_{\mathcal{K}}[J^{MN}] \leq \Pi_M, \quad (44) \end{aligned}$$

where we have an independent SDP for each actual state and POVM element indexed by i, \tilde{n} and j , respectively.

In some cases, it is more convenient to perform a relaxed version of this generalized decoy-state analysis that does not involve the preparation channels Ξ_i as follows. Consider the set of infinite-dimensional SDPs described in Eq. (14)

$$\begin{aligned} & \text{opt.}_J \text{Tr}[(\Xi_i(|\tilde{n}\rangle\langle\tilde{n}|))^T \otimes F_j]J \\ & \text{such that } \text{Tr}[(\Xi_k(\rho^\mu))^T \otimes \Gamma_l]J = \gamma_{|k, \mu} \quad \forall k, l, \mu \\ & J \geq 0 \\ & \text{Tr}_{\mathcal{K}}[J] = \mathbb{I}_{\mathcal{H}}, \quad (45) \end{aligned}$$

where we have made the dependence of the actual and virtual states on the preparation channels Ξ_i explicit. Recall

that the constraints are equivalent to J being the Choi isomorphism of a channel Φ . So Eq. (45) is equivalent to

$$\begin{aligned} & \text{opt.}_{\Phi} \text{Tr} [F_j \Phi (\Xi_i (|\tilde{n}\rangle \langle \tilde{n}|))] \\ & \text{such that } \text{Tr} [\Gamma_l \Phi (\Xi_k (\rho^\mu))] = \gamma_{j|k,\mu} \quad \forall k, l, \mu \quad (46) \\ & \Phi \text{ is CPTP.} \end{aligned}$$

Two relaxations can now simplify these optimization problems:

- (1) Ignoring all constraints where $k \neq i$.
- (2) Taking $\Phi' = \Phi \circ \Xi_i$ to be the new optimization variable. Note that since the composition of two channels is also a channel, Φ' is also a channel.

This expands the set being optimized over as we no longer fix Ξ_i as can be seen by writing the resulting set of optimization problems

$$\begin{aligned} & \text{opt.}_{\Phi'} \text{Tr} [F_j \Phi' (|\tilde{n}\rangle \langle \tilde{n}|)] \\ & \text{such that } \text{Tr} [\Gamma_l \Phi' (\rho^\mu)] = \gamma_{j|i,\mu} \quad \forall l, \mu \quad (47) \\ & \Phi' \text{ is CPTP.} \end{aligned}$$

Since these relaxations expand the feasible set, the max (min) will be upper (lower) bounds of the original SDPs given in Eq. (45).

Rewriting this as an SDP using the Choi matrix formalism we get

$$\begin{aligned} & \text{opt.}_J \text{Tr} [(|\tilde{n}\rangle \langle \tilde{n}|^T \otimes F_j) J] \\ & \text{such that } \text{Tr} [(\rho^{\mu T} \otimes \Gamma_l) J] = \gamma_{l|i,\mu} \quad \forall l, \mu \quad (48) \\ & J \geq 0 \\ & \text{Tr}_{\mathcal{K}} [J] = \mathbb{I}_{\mathcal{H}}. \end{aligned}$$

Finally, use the results stated in Sec. IV C to replace Eq. (48) with the finite-dimensional SDP

$$\begin{aligned} Y_{\tilde{n}}(i, j) &= \text{opt.}_{J^{MN}} \text{Tr} \left[\left(\sigma_{\tilde{n}}^M \otimes F_j^N \right) J^{MN} \right] \\ & \text{such that } \text{Tr} \left[\left(\rho^{\mu M T} \otimes \Gamma_l^N \right) J^{MN} \right] \leq \gamma_{l|i,\mu} + \epsilon_M^\mu \\ & \text{Tr} \left[\left(\rho^{\mu M T} \otimes \Gamma_l^N \right) J^{MN} \right] \\ & \geq \gamma_{l|i,\mu} - W_{iN}^\mu - w_M^\mu - 2\epsilon_M^\mu \quad \forall l, \mu \\ & J^{MN} \geq 0 \\ & \text{Tr}_{\mathcal{K}} [J^{MN}] \leq \Pi_M, \quad (49) \end{aligned}$$

where $\sigma_{\tilde{n}} := |\tilde{n}\rangle \langle \tilde{n}|$.

For some preparation channels, the dimension of the SDPs in Eq. (49) are smaller than the dimensions of the SDPs in Eq. (44) for the same $w_{kM}^\mu = w_M^\mu$. An example where this is the case is the three-state protocol described in Sec. VI. Thus, it is sometimes advantageous to relax the problem to the more computationally tractable SDPs described in Eq. (49).

V. APPROXIMATE DIAGONALIZATION

The eigendecomposition shown in Eq. (43) is crucial for block tagging and generalized decoy-state analysis. The eigenvalues $p_{\tilde{n}}$ are used in the objective function of Eq. (4). The eigenvectors $|\tilde{n}\rangle$ are used in Eq. (4) when determining $\rho_A^{\tilde{n}}$ for the partial trace constraint, and in Eqs. (44) or (49) when determining $\sigma_{i,\tilde{n}}$ or $\sigma_{\tilde{n}}$, respectively.

Unfortunately, the eigendecomposition might be hard to find exactly as these are infinite-dimensional operators that cannot be numerically diagonalized. However, the eigendecomposition of a finite projection can be numerically found. This motivates the following definitions. Let ρ represent the infinite-dimensional density operator whose eigendecomposition we would like to estimate. Define $\rho' = \rho^\Pi + \rho^{\bar{\Pi}}$ where $\rho^\Pi = \Pi \rho \Pi$ and $\rho^{\bar{\Pi}} = \bar{\Pi} \rho \bar{\Pi}$ for some finite projection Π .

Note that ρ^Π can be numerically diagonalized, and this would constitute a subset of the eigenvalues and eigenvectors of ρ' . How closely the eigendecomposition of ρ' will estimate the eigendecomposition of ρ depends on the choice of projection Π . A useful choice of Π would be one where the off-diagonal blocks are ‘‘almost’’ 0 so that intuitively the eigendecomposition ρ^Π is ‘‘nearly’’ that of ρ . This is formalized in the following theorem whose proof is given in Appendix B 5.

Theorem 6.—Let $\rho = \sum_{\tilde{n}} p_{\tilde{n}} |\tilde{n}\rangle \langle \tilde{n}|$ where $p_0 \geq p_1 \geq \dots$, and ρ' have eigendecomposition

$$\rho' = \sum_{\tilde{n}} p'_{\tilde{n}} |v_{\tilde{n}}\rangle \langle v_{\tilde{n}}|, \quad (50)$$

where $p'_0 \geq p'_1 \geq \dots$. Define $\delta_{\tilde{n}} := \min\{p'_n - p'_{n-1} - \epsilon_{\text{proj}}, p'_{n+1} - p'_n - \epsilon_{\text{proj}}\}$ where $\epsilon_{\text{proj}} := \left\| \sqrt{\rho^{\Pi^g}} \Pi \rho \bar{\Pi} \sqrt{\rho^{\bar{\Pi}^g}} \right\|_\infty \sqrt{\text{Tr}[\rho^{\bar{\Pi}}]}$. Then

- (1) $|p'_n - p_{\tilde{n}}| \leq \epsilon_{\text{proj}}$, and
- (2) $F(|v_{\tilde{n}}\rangle \langle v_{\tilde{n}}|, |\tilde{n}\rangle \langle \tilde{n}|)^2 \geq 1 - \frac{\epsilon_{\text{proj}}^2}{\delta_{\tilde{n}}^2}$.

Using Fuchs-van de Graaf inequality [35] along with Theorem 6, we get

$$\| |v_{\tilde{n}}\rangle \langle v_{\tilde{n}}| - |\tilde{n}\rangle \langle \tilde{n}| \|_1 \leq 2\epsilon_{\text{proj}}/\delta_{\tilde{n}}. \quad (51)$$

For notational convenience, we define this quantity to be $\epsilon_{\text{vec}}^{\tilde{n}} := 2\epsilon_{\text{proj}}/\delta_{\tilde{n}}$. We can use Theorem 6 for QKD to

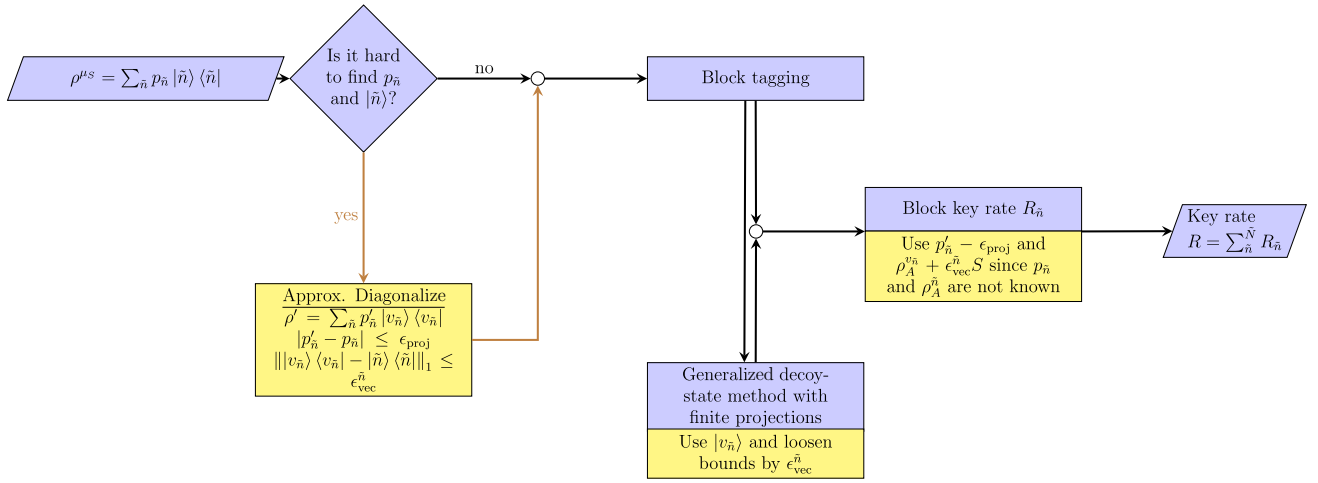


FIG. 4. Flowchart depicting the application of the generalized decoy-state method to QKD. The yellow parts denote the modifications to be made if we need to approximately diagonalize the density operator.

approximately diagonalize ρ^{μ_s} as defined in Eq. (43). This approximate diagonalization would lead to minor modifications to the the generalized decoy-state bounds, as well as the key-rate SDP as depicted in Fig. 4.

A. Approximate generalized decoy-state analysis

We first describe the use of Eq. (51) in obtaining bounds on the generalized decoy-state SDP given in Eq. (44), where $|\tilde{n}\rangle$ appears in the objective function. By numerically diagonalizing $\Pi\rho^{\mu_s}\Pi$, we can find $\sigma_{v_{\tilde{n}}} = |v_{\tilde{n}}\rangle\langle v_{\tilde{n}}|$. This can be used instead of $|\tilde{n}\rangle$ to construct the virtual states for the objective function in Eq. (44). Let the optimal values of the modified SDP be denoted by $Y_{v_{\tilde{n}}}(i, j)$. The optimal values of the original SDPs $Y_{\tilde{n}}(i, j)$ can be related to the optimal values of the modified SDPs $Y_{v_{\tilde{n}}}(i, j)$ by using the result in Eq. (51) with Hölder's inequality to get

$$|Y_{\tilde{n}}(i, j) - Y_{v_{\tilde{n}}}(i, j)| \leq \epsilon_{\text{vec}}^{\tilde{n}}. \quad (52)$$

Recall that the generalized decoy-state analysis makes use of finite projections Π_M on the virtual state $\sigma_{v_{\tilde{n}}}$. This results in an additional ϵ_{iM} cost as described in Theorem 4. By choosing $\Pi \geq \Pi_M$, we can ensure that $\sigma_{v_{\tilde{n}}} = \Pi_M \sigma_{v_{\tilde{n}}} \Pi_M$ resulting in a reduced cost $\epsilon_{iM} = 0$. Thus, this suggests prudent choices for the different finite projections used in our analysis.

B. Approximate key-rate SDP

The eigenvectors $|\tilde{n}\rangle$ appear in the key-rate SDP in Eq. (4) in the partial trace constraint $\text{Tr}_B[\rho_{AB}^{\tilde{n}N}] \leq \rho_A^{\tilde{n}}$, and in the bounds $Y_{\tilde{n}}(i, j)$. The eigenvalues $p_{\tilde{n}}$ appear in Eq. (4) as a prefactor to the objective function. We use the approximate eigenvectors $|v_{\tilde{n}}\rangle$ and eigenvalues $p_{\tilde{n}}$ to construct a similar SDP that bounds the key rate.

Corollary 6.1.—

$$\begin{aligned} R_{\tilde{n}}^N &\geq \min_{\rho_{AB}^{\tilde{n}N}} (p'_{\tilde{n}} - \epsilon_{\text{proj}}) f(\rho_{AB}^{\tilde{n}N}) \\ &\text{s.t. } Y_{v_{\tilde{n}}}^L(i, j) - \epsilon_{\text{vec}}^{\tilde{n}} \\ &\leq \text{Tr} \left[\Gamma_j^N \Phi(\rho_i^{\tilde{n}}) \right] \leq Y_{v_{\tilde{n}}}^U(i, j) + \epsilon_{\text{vec}}^{\tilde{n}} \\ \text{Tr}_B \left[\rho_{AB}^{\tilde{n}N} \right] &\leq \rho_A^{v_{\tilde{n}}} + \epsilon_{\text{vec}}^{\tilde{n}} S \\ \|S\|_1 &\leq 1 \\ 1 - W_{\tilde{n}} - \epsilon_{\text{vec}}^{\tilde{n}} &\leq \text{Tr} \left[\rho_{AB}^{\tilde{n}N} \right] \leq 1 \\ S &\geq 0 \\ \rho_{AB}^{\tilde{n}N} &\geq 0, \end{aligned} \quad (53)$$

where $R_{\tilde{n}}^N$ is defined in Eq. (4).

Proof.—We first prove that any feasible $\rho_{AB}^{\tilde{n}N}$ for the SDP in Eq. (4) is also feasible for the SDP in Eq. (53). That

$$Y_{v_{\tilde{n}}}^L(i, j) - \epsilon_{\text{vec}}^{\tilde{n}} \leq \text{Tr} \left[\Gamma_j^N \Phi(\rho_i^{\tilde{n}}) \right] \leq Y_{v_{\tilde{n}}}^U(i, j) + \epsilon_{\text{vec}}^{\tilde{n}}$$

is implied by

$$Y_{\tilde{n}}^L(i, j) \leq \text{Tr} \left[\Gamma_j^N \Phi(\rho_i^{\tilde{n}}) \right] \leq Y_{\tilde{n}}^U(i, j)$$

is a direct consequence of Eq. (52).

Given that $\text{Tr}_B[\rho_{AB}^{\tilde{n}N}] \leq \rho_A^{\tilde{n}}$, we aim to show that

$$\text{Tr}_B \left[\rho_{AB}^{\tilde{n}N} \right] \leq \rho_A^{v_{\tilde{n}}} + \epsilon_{\text{vec}}^{\tilde{n}} S,$$

where S is a positive semidefinite operator with $\|S\|_1 \leq 1$. Recall from Eq. (1) that

$$|\psi^{\tilde{n}}\rangle_{AA'} = \sum_i \sqrt{p(i)} |i\rangle_A \otimes V_i |\tilde{n}\rangle_{A'}, \quad (54)$$

$$|\psi^{v_{\tilde{n}}}\rangle_{AA'} = \sum_i \sqrt{p(i)} |i\rangle_A \otimes V_i |v_{\tilde{n}}\rangle_{A'}, \quad (55)$$

where V_i is the isometry that define the isometric preparation channels Ξ_i . As a direct consequence of Theorem 6 we get

$$F(\rho_{AA'}^{\tilde{n}}, \rho_{AA'}^{v_{\tilde{n}}}) = F(|v_{\tilde{n}}\rangle\langle v_{\tilde{n}}|, |\tilde{n}\rangle\langle \tilde{n}|) \quad (56)$$

$$\geq \sqrt{1 - \frac{\epsilon_{\text{proj}}^2}{\delta_{\tilde{n}}^2}}, \quad (57)$$

where $\rho_{AA'}^{\tilde{n}} = |\psi^{\tilde{n}}\rangle\langle \psi^{\tilde{n}}|_{AA'}$ and $\rho_{AA'}^{v_{\tilde{n}}} = |\psi^{v_{\tilde{n}}}\rangle\langle \psi^{v_{\tilde{n}}}|_{AA'}$.

Thus, Fuchs-van de Graaf inequality can be used to obtain

$$\left\| \rho_{AA'}^{\tilde{n}} - \rho_{AA'}^{v_{\tilde{n}}} \right\|_1 \leq \epsilon_{\text{vec}}^{\tilde{n}}. \quad (58)$$

Since the partial trace channel can only decrease the 1-norm, this gives

$$\left\| \rho_A^{\tilde{n}} - \rho_A^{v_{\tilde{n}}} \right\|_1 \leq \epsilon_{\text{vec}}^{\tilde{n}}. \quad (59)$$

Thus, the partial trace constraint $\text{Tr}_B [\rho_{AB}^{\tilde{n}N}] \leq \rho_A^{\tilde{n}}$ implies

$$\text{Tr}_B [\rho_{AB}^{\tilde{n}N}] \leq \rho_A^{v_{\tilde{n}}} + \epsilon_{\text{vec}}^{\tilde{n}} S, \quad (60)$$

where S is a positive semidefinite operator with $\|S\|_1 \leq 1$.

Thus, the feasible set for the SDP in Eq. (53) contains the feasible set for the SDP in Eq. (4). Finally, Theorem 6 states that

$$p_{\tilde{n}} \geq p'_{\tilde{n}} - \epsilon_{\text{proj}}$$

completing the proof. \blacksquare

VI. THREE-STATE PROTOCOL

We shall now apply the methods developed so far to analyze the effects of imperfect phase randomization on the key rate of the time-bin encoded three-state protocol. This protocol can be implemented primarily by using passive components, which are easy to manufacture. A recent implementation [36] was able to share secret keys over 421 km under the assumption that the laser is fully phase randomized. However, the 2.5-GHz laser used in the implementation did not perfectly randomize the phase [17] highlighting the significance of the methods developed in this paper.

A. Protocol description

1. State preparation

Alice produces a laser pulse with some phase distribution as described in Eq. (5). She then passes it through an unbalanced Michelsons interferometer that transforms the coherent state from $|\alpha\rangle \rightarrow |\alpha/2\rangle \otimes |\alpha/2\rangle$. Alice randomly chooses a bit to encode from $\{0, 1, +\}$ with an *a priori* probability distribution and transforms the state accordingly:

- 0: Alice uses an intensity modulator to suppress the first pulse.
- 1: Alice uses an intensity modulator to suppress the second pulse.
- +: Alice uses a variable attenuator to halve the intensity of each pulse so that the total mean photon number of both pulses in all 3 states are the same.

Additionally Alice uses the variable attenuator to send some decoy states with different intensities with the same encoding as the signal states.

2. Measurement

Bob's basis choice is made passively via a beam splitter. The Z -basis detection is made by a threshold detector that measures the time of arrival. This measurement is used for key generation. The X -basis detection is made via a Mach-Zehnder interferometer that measures the coherences between pulses. Here, only the “-” detector is used for experimental simplicity. The setup is shown in Fig. 5.

3. Simulation parameters

The laser visibility was measured [17] to be $V = 0.0019$. In order to interpret this measurement result as the degree of phase randomization q , we need to make model assumptions on the general laser state as discussed in Sec. III B. For the two physical model assumptions discussed in Sec. III B, we get $q \approx 0.9564$ when we assume $p_{\Phi_i}(\phi_i) = (q/2\pi) + (1-q)\delta(\phi_i)$, and $q \approx 0.9128$ when $p_{\Phi_i}(\phi_i)$ is a wrapped normal distribution.

The channel is modeled as a loss-only channel with a low attenuation of 0.16 dB/km based on the implementation in Ref. [36]. We reduce the number of constraints to speed up computation time. In particular, we consider no-click events, single-click events, and group all multiclick events together as a single event. Bob's threshold detectors are assumed to be ideal without any dark counts or loss.

Ideally, we would want to optimize over all free parameters to maximize the key rate we can produce. However, this is computationally very taxing and so we pick some fixed arbitrary values for the free parameters. Thus, our results deliver provable secure key rates, but we do not

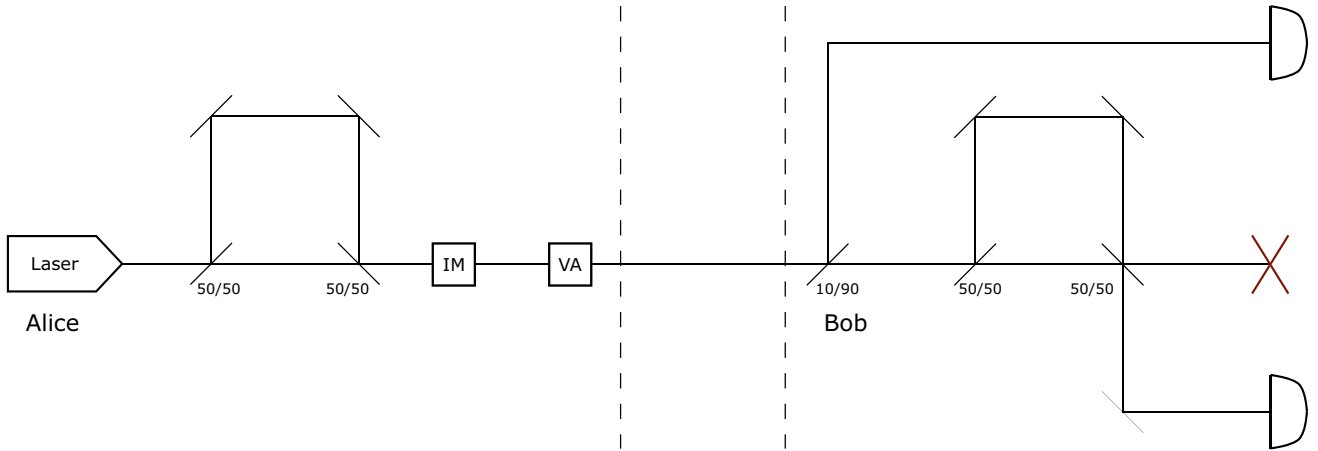


FIG. 5. Schematics of the implementation of the three-state protocol as in Ref. [36]. The numbers below the beam splitters reflect their transmissivity. IM and VA refer to intensity modulator and variable attenuator, respectively.

claim optimality. Alice's states are all chosen with equal *a priori* probabilities. The decoy amplitudes used are 0 and 0.5 while the signal intensity is optimized for different distances. Bob's passive beam splitter is a 0.9/0.1 beam splitter with the 0.9 being towards the Z-basis choice.

B. Applying generalized decoy-state analysis

The laser is characterized as described in Sec. III B to obtain values for the degree of phase randomization q . Using this parameter with the source map described in Sec. III A we reduce the general problem to finding the key rate given Alice's prepared states $\rho_i^\mu = \Xi_i(\rho_{\text{model}}^\mu)$. Note that since the three states have the same mean photon number, the preparation channels Ξ_i can be represented by isometric channels by choosing the base state to also have the same mean photon number. We can now follow the process depicted in Fig. 4 to obtain the key rate for these states.

This first step is to approximately diagonalize $\rho_{\text{model}}^{\mu_S}$ where μ_S is the signal intensity. We take a finite projection in photon-number space upto d photons Π_d to numerically diagonalize the operator. Let $|v_{\bar{n}}\rangle$ and $\lambda_{\bar{n}}$ be the resulting eigenvectors and eigenvalues. Using Theorem IX.5.9 from Ref. [37] along with the fact that

$$\rho_{\text{model}}^{\mu_S} = q \sum_{n=0}^{\infty} e^{-\mu_S} \frac{\mu_S^n}{n!} |n\rangle\langle n| + (1-q) |\sqrt{\mu_S}\rangle\langle\sqrt{\mu_S}| \quad (61)$$

is positive semidefinite for all $q \in [0, 1]$, we can conclude that

$$\left\| \sqrt{\Pi_d \rho_{\text{model}}^{\mu_S} \Pi_d}^g \Pi_d \rho_{\text{model}}^{\mu_S} \Pi_d \sqrt{\Pi_d \rho_{\text{model}}^{\mu_S} \Pi_d}^g \right\|_{\infty} \leq (1-q).$$

$w_d^\mu = \text{Tr}[\rho^\mu \bar{\Pi}_d]$ is given by $w_d^\mu = 1 - \sum_{n=0}^d e^{-\mu} (\mu^n/n!)$. The relevant bounds $\epsilon_{\text{proj}}^{\mu_S}$ and $\epsilon_{\text{vec}}^{\mu_S \bar{n}}$ can then be found for the state $\rho_{\text{model}}^{\mu_S}$ to use the results shown in Sec. V. Note that these calculations are more general than the three-state protocol, and can be used for *any* protocol with imperfect phase randomisation. We can also block-tag the signal state given in Eq. (61) as shown in Sec. II C to choose the relevant virtual states for the decoy-state analysis.

We can then use the generalised decoy-state SDP as described in Sec. IV D. In order to save computational time, we use the reduction given in Eq. (49). We choose to project onto the space with less than or equal to N photons in both pulses Π_N when considering the measurement space. This commutes with all the POVM elements Γ_j since they are all threshold detectors. The projection on the state space Π_M is chosen to be the same as the projection used for approximate diagonalisation Π_d . Thus, $\Pi_M \leq \Pi_d$ and $\sigma_{\bar{n}} = |v_{\bar{n}}\rangle\langle v_{\bar{n}}|$ already lives entirely within the space spanned by Π_M . So the correction term described in Theorem 4 goes to 0. Additionally, $w_M^\mu = w_d^\mu$.

To apply Eq. (49) the quantities ϵ_M^μ and W_{iN}^μ still need to be computed. ϵ_M^μ can be bound as described in Lemma 2 as $\epsilon_M^\mu \leq (1-q)w_M^\mu$. It is possible to bound W_{iN}^μ from our observations as shown in Appendix C. This fully defines the finite dimensional SDPs shown in Eq. (49) that can be numerically solved. The solutions of these SDPs together with the other parameters can be used to define the key rate SDP shown in Eq. (53). This gives us a lower bound on the key rate.

C. Results

We compared the key rate of the protocol with different degrees of partial phase-randomisation $q = 0.9128$ and $q = 0.9564$, and perfect phase-randomisation $q = 1$ as is shown in Fig. 6. We observe that the key rates for

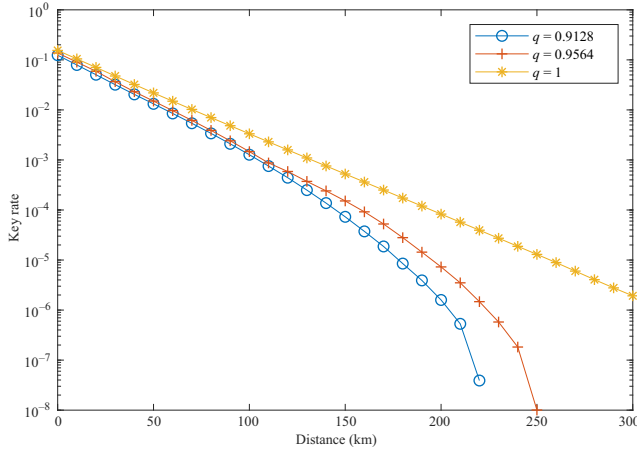


FIG. 6. Comparison of the key rate of the three-state protocol with partial and complete phase randomization.

the incomplete phase-randomized lasers vary significantly from the key rate for the fully phase-randomized laser. This highlights the usefulness of experimentally characterizing the degree of phase randomization q for high-speed QKD experiments, and using q with our proof techniques to calculate the secret key rate.

The use of numerics in our methods leave some room for looseness in our results. Take for instance the bound $\epsilon_{\text{vec}}^{\mu, S^n}$ on the closeness of the approximate eigenvectors to the true eigenvectors described in Sec. V. This bound is limited by machine precision, as we choose the dimension d to project onto to be large enough that w_d^μ can be upper bounded by the machine precision. Thus, the key rate for the imperfectly phase-randomized states can be brought closer to the fully phase-randomized key rates by increasing the machine precision. Additionally, since we use the same projection while using the generalized decoy-state methods, the machine precision would also loosen the constraints in Eq. (49) through ϵ_M^μ .

VII. CONCLUSION

In this paper, we developed two QKD proof techniques in order to accommodate imperfect phase randomization into security proofs. The first was the source-map construction in Sec. III A to reduce the security for independent pulses to the security of an IID source. This reduction crucially requires the characterization of the degree of phase randomization q . However, the experimental characterization of this quantity is still a key open problem. Moreover we numerically display the effect of improper characterization on the key rate in Fig. 6. Thus, we believe that future work should focus on estimating q experimentally.

The second proof technique is the generalized decoy-state analysis introduced in Sec. IV. This allows us to perform a decoy-state analysis with any IID characterized source. Thus, in conjunction with the source map this

allows us to perform a decoy-state security proof of imperfectly phase-randomized laser sources. Moreover, these techniques are more general and can be applied outside decoy-state QKD, for example, to bound the statistics of cat states in Ref. [34].

Although we have computed the key rates of the three-state protocol motivated by the partial characterization of the experimental setup in Ref. [17], we emphasize that all our proof methods can be directly applied to any decoy-state QKD protocol. In specifics, they can be applied to MDI QKD [38,39] or twin-field QKD [40,41]. Dealing with source imperfections in these protocols is of particular relevance as the only side-channel attacks concern the sources. Thus, a step toward performing decoy-state analysis in the presence of imperfections would be to combine the results from this work and Ref. [15] on phase imperfections, with the work done in Ref. [12,13] on intensity correlations. This can then be combined with the results in Refs. [6–8] on qubit imperfections to obtain secure key rates against arbitrary source imperfections.

ACKNOWLEDGMENTS

We thank Marcos Curty and Guillermo Currás-Lorenzo for insightful discussions regarding Ref. [15]. The work has been performed at the Institute for Quantum Computing, at the University of Waterloo, which is supported by Innovation, Science, and Economic Development Canada. The research has been supported by NSERC under the Discovery Grants Program, Grant No. 341495.

APPENDIX A: PROOFS RELATED TO SOURCE MAPS

In this Appendix, we formally prove some results about source maps stated in the main text.

1. Using source maps to lower bound the key rate

Throughout the paper, we have heavily relied on the idea of source maps. As intuitively explained in Sec. II C, the existence of a source map can be used to lower bound the key rate of a protocol with virtual states.

We first set up some notation before formally stating and proving the theorem. Alice's prepared state can be written as $\rho_{AA'} = \sum_{i,\mu} |i, \mu\rangle\langle i, \mu| \otimes \rho_i^\mu$ where A' is the system sent to Bob through the insecure quantum channel Φ . Let $V_\Phi : A' \rightarrow BE$ be the Stinespring representation of Φ so that the state shared by Alice, Bob, and Eve can be written as

$$\rho_{ABE} = \sum_{i,\mu} |i, \mu\rangle\langle i, \mu| \otimes \left(V_\Phi \rho_i^\mu V_\Phi^\dagger \right). \quad (\text{A1})$$

Let $\Delta : AB \rightarrow YZC$ be the protocol map that maps the joint state held by Alice and Bob to the raw key Z ,

Bob's measurement outcomes Y along with the public announcements C in that round. Thus,

$$\rho_{YZCE} = (\Delta \otimes \mathbb{I}_{E \rightarrow E}) (\rho_{ABE}). \quad (\text{A2})$$

The key rate can be given by the Devetak-Winter formula

$$R_\rho^\infty = \min_{\Phi \in \mathcal{C}_{\text{real}}} H(Z | CE) - \delta_{\text{leak}}, \quad (\text{A3})$$

where $\mathcal{C}_{\text{real}}$ is the set of channels compatible with Alice and Bob's observed statistics, and ρ_{YZCE} is as defined in Eq. (A2). Note that E is the auxiliary system corresponding to the Stinespring representation of the channel Φ . So defining Φ specifies E upto local unitaries. We formally show that the key rate R_ρ^∞ of the real protocol with signal states $\{\rho_i\}$ can be lower bounded by using a source map as stated in Sec. II C.

Theorem 7 (Source-map key rate).—Define a virtual protocol with the same statistics as the real protocol, where Alice prepares the states $\{\tau_i\}$ with asymptotic key rate R_τ^∞ . Let Ψ be a source map connecting the virtual states to the real states such that $\rho_i = \Psi(\tau_i)$ for all i . Then $R_\tau^\infty \leq R_\rho^\infty$.

Proof.—The key rate of the virtual protocol is given by

$$R_\tau^\infty = \min_{\Phi_{\text{vir}} \in \mathcal{C}_{\text{vir}}} H(Z | CE_{\text{vir}}) - \delta_{\text{leak}}, \quad (\text{A4})$$

where

$$\rho_{YZCE_{\text{vir}}} = (\Delta \otimes \mathbb{I}_{E_{\text{vir}} \rightarrow E_{\text{vir}}}) \times \left(\sum_{i,\mu} |i, \mu\rangle\langle i, \mu| \otimes \left(V_{\Phi_{\text{vir}}} \tau_i^\mu V_{\Phi_{\text{vir}}}^\dagger \right) \right) \quad (\text{A5})$$

and \mathcal{C}_{vir} is the set of channels compatible with Alice and Bob's observed statistics. Let $\mathcal{C}_\Psi := \{\Phi_{\text{vir}} | \Phi_{\text{vir}} = \Phi \circ \Psi, \Phi \in \mathcal{C}_{\text{real}}\}$.

Since the virtual protocol has the same statistics as the real protocol, \mathcal{C}_Ψ is compatible with Alice and Bob's observed statistics. As a result $\mathcal{C}_\Psi \subset \mathcal{C}_{\text{vir}}$. Additionally, it is straightforward to see that for every $\Phi \in \mathcal{C}_{\text{real}}$, there exists a $\Phi_{\text{vir}} \in \mathcal{C}_\Psi$. Thus, minimizing over a smaller set of channels, can only increase the optimal value,

$$\begin{aligned} R_\tau^\infty &\leq \min_{\Phi_{\text{vir}} \in \mathcal{C}_\Psi} H(Z | CE_{\text{vir}}) - \delta_{\text{leak}} \\ &= \min_{\Phi \in \mathcal{C}} H(Z | CE_{\text{vir}}) - \delta_{\text{leak}}, \end{aligned} \quad (\text{A6})$$

where Eq. (A6) follows from the identification between $\mathcal{C}_{\text{real}}$ and \mathcal{C}_Ψ made above.

Let $V_\Psi : A'' \rightarrow A'E_{\text{sou}}$ be the Stinespring representation of the source map Ψ such that

$$\rho_{ABEE_{\text{sou}}} = \sum_{i,\mu} |i, \mu\rangle\langle i, \mu| \otimes \left(V_\Phi V_\Psi \tau_i^\mu V_\Psi^\dagger V_\Phi^\dagger \right), \quad (\text{A7})$$

where E_{vir} has been explicitly broken up into the individual auxiliary systems E and E_{sou} of Φ and Ψ , respectively. Thus, it follows that $\rho_{ABE} = \text{Tr}_{E_{\text{sou}}} [\rho_{ABEE_{\text{sou}}}]$.

The protocol map Δ is identical for both the virtual and real protocols. Additionally, the output ρ_{YZC} of the protocol map is also identical since the statistics for both protocols are identical. Thus, $\rho_{YZCE} = \text{Tr}_{E_{\text{sou}}} [\rho_{YZCEE_{\text{sou}}}]$ for all $\rho_{YZCEE_{\text{sou}}}$ corresponding to channels $\Phi_{\text{vir}} \in \mathcal{C}_\Psi$. The strong subadditivity of the conditional von Neumann entropies [42] combined with Eq. (A6) gives us the required inequality

$$\begin{aligned} R_\tau^\infty &\leq \min_{\Phi_{\text{vir}} \in \mathcal{C}_\Psi} H(Z | CEE_{\text{sou}}) - H(Z | Y) \\ &\leq \min_{\Phi_{\text{vir}} \in \mathcal{C}_\Psi} H(Z | CE) - H(Z | Y) \\ &= \min_{\Phi \in \mathcal{C}} H(Z | CE) - H(Z | Y) = R_\rho^\infty. \end{aligned} \quad (\text{A8})$$

■

2. Construction of physical map connecting model laser state to actual laser state

Define the following for notational convenience:

$$\rho_\phi := |\sqrt{\mu} \exp\{i\phi}\rangle\langle\sqrt{\mu} \exp\{i\phi}\|, \quad (\text{A9})$$

$$U_\theta : |\sqrt{\mu} \exp\{i\phi}\rangle \mapsto |\sqrt{\mu} \exp\{i\phi + \theta\}\rangle, \quad (\text{A10})$$

where U_θ represents the action of a phase modulator, which is unitary. Let $\rho_{\text{PR}} = \int_0^{2\pi} d\phi (1/2\pi) \rho_\phi$ be the fully phase-randomized state and $\rho_{\text{model}} = q\rho_{\text{PR}} + (1-q) |\sqrt{\mu}\rangle\langle\sqrt{\mu}|$. Also define

$$\tau_\phi := U_\phi \rho_{\text{model}} U_\phi^\dagger, \quad \text{and} \quad (\text{A11})$$

$$\tilde{p}_{\Phi_1 \dots \Phi_n}(\phi_1 \dots \phi_n) := \tilde{p}_{\Phi_1}(\phi_1) \dots \tilde{p}_{\Phi_n}(\phi_n | \phi_1 \dots \phi_{n-1}), \quad (\text{A12})$$

where $\tilde{p}_{\Phi_i}(\phi_i | \phi_1 \dots \phi_{i-1}) := \frac{p_{\Phi_i}(\phi_i | \phi_1 \dots \phi_{i-1}) - q/2\pi}{1-q}$.

Lemma 8.—Define

$$\begin{aligned} \Phi(\sigma^n) &:= \int_0^{2\pi} \dots \int_0^{2\pi} d\phi_1 \dots d\phi_n \tilde{p}_{\Phi_1 \dots \Phi_n}(\phi_1 \dots \phi_n) \\ &\times (U_{\phi_1} \dots U_{\phi_n}) \sigma^n (U_{\phi_1}^\dagger \dots U_{\phi_n}^\dagger). \end{aligned} \quad (\text{A13})$$

Then

(1) If $q \leq 2\pi \min_i \min_{\phi_i} p_{\Phi_i}(\phi_i | \phi_1 \dots \phi_{i-1})$, then Φ is a mixed unitary channel.

(2) If the actual laser state is phase-independent across pulses, i.e., $p_{\Phi_i}(\phi_i | \phi_1 \dots \phi_{i-1}) = p_{\Phi_i}(\phi_i)$ for all i , then

$$\Phi(\rho_{\text{model}}^{\otimes n}) = \rho_{\text{laser}}$$

where ρ_{laser} is as defined in Eq. (5).

Proof.—Condition (1).

Verifying that \tilde{p} is a probability density function is straightforward. This directly implies that Φ is a mixed unitary channel.

Condition (2).

First note that $U_{\phi_i} \rho_{\text{PR}} U_{\phi_i}^\dagger = \rho_{\text{PR}}$ for all $\phi_i \in [0, 2\pi)$ where ρ_{PR} is the fully phase-randomized state. Using this, a straightforward computation gives

$$\begin{aligned} & \int_0^{2\pi} d\phi_i \tilde{p}_{\Phi_i}(\phi_i | \phi_1 \dots \phi_{i-1}) \tau_{\phi_i} \\ &= \int_0^{2\pi} d\phi_i p_{\Phi_i}(\phi_i | \phi_1 \dots \phi_{i-1}) \rho_{\phi_i}. \end{aligned} \quad (\text{A14})$$

Now looking at the action of the map on the model state,

$$\begin{aligned} \Phi(\rho_{\text{model}}^{\otimes n}) &= \int_0^{2\pi} \dots \int_0^{2\pi} d\phi_1 \dots d\phi_n \\ &\quad \times \tilde{p}_{\Phi_1 \dots \Phi_n}(\phi_1 \dots \phi_n) \\ &\quad \times (U_{\phi_1} \dots U_{\phi_n}) \rho_{\text{model}}^{\otimes n} (U_{\phi_1}^\dagger \dots U_{\phi_n}^\dagger) \end{aligned} \quad (\text{A15})$$

$$\begin{aligned} &= \int_0^{2\pi} d\phi_1 \tilde{p}_{\Phi_1}(\phi_1) \tau_{\phi_1} \otimes \dots \\ &\quad \otimes \int_0^{2\pi} d\phi_n \tilde{p}_{\Phi_n}(\phi_n) \tau_{\phi_n} \end{aligned} \quad (\text{A16})$$

$$\begin{aligned} &= \int_0^{2\pi} d\phi_1 p_{\Phi_1}(\phi_1) \rho_{\phi_1} \otimes \dots \\ &\quad \otimes \int_0^{2\pi} d\phi_n p_{\Phi_n}(\phi_n) \rho_{\phi_n} \end{aligned} \quad (\text{A17})$$

$$\begin{aligned} &= \int_0^{2\pi} \dots \int_0^{2\pi} d\phi_1 \dots d\phi_n p_{\Phi_1 \dots \Phi_n} \\ &\quad \times (\phi_1 \dots \phi_n) \rho_{\phi_1} \otimes \dots \otimes \rho_{\phi_n} \end{aligned} \quad (\text{A18})$$

$$= \rho_{\text{laser}}, \quad (\text{A19})$$

where Eq. (A16) follows from the assumption that the probability distribution is independent, and Eq. (A17) follows from Eq. (A14). ■

Note that the independence condition was crucial for this channel to reproduce the actual laser state. Specifically, Eq. (A17) would not hold for a correlated probability

distribution. Thus, this technique cannot directly be used to reduce phase-correlated laser states to IID states. The reduction from phase-correlated laser states to an independent laser state has been done in Ref. [15], and we thank the authors for pointing out this limitation in our methods.

APPENDIX B: BOUNDS ON PROJECTED OPERATORS

In this Appendix we give the derivations for various results on projected operators that we use in Sec. IV C.

1. Bounds on 1-norm

In this Appendix we derive some useful bounds that will be used to prove the results in the rest of Appendix B. To set up notation, let ρ be a density matrix, Π be a projection with orthogonal complement $\bar{\Pi} := \mathbb{I} - \Pi$, and $\rho^\Pi = \Pi \rho \Pi$. Using Eqs. (59) and (60) in the proof of Lemma 5 from Ref. [43], we get $\|\Pi \rho \bar{\Pi}\|_1 \leq \sqrt{1 - \text{Tr}[\rho^\Pi]}$. For notational convenience, let $W := 1 - \text{Tr}[\rho^\Pi]$ so that we can write

$$\|\Pi \rho \bar{\Pi}\|_1 \leq \sqrt{W}. \quad (\text{B1})$$

Note that the bound in Eq. (B1) depends only on $\text{Tr}[\rho^\Pi]$. Borrowing intuition from Lemma 4 of Ref. [33], we would expect this bound to be tighter when the state is closer to block diagonal. Thus, we tighten the bound as follows.

Theorem 9.—Let ρ be a density matrix. With respect to a projection Π , write ρ as a block-diagonal matrix

$$\rho = \begin{pmatrix} \Pi \rho \Pi & \Pi \rho \bar{\Pi} \\ \bar{\Pi} \rho \Pi & \bar{\Pi} \rho \bar{\Pi} \end{pmatrix} = \begin{pmatrix} A & B \\ B^\dagger & D \end{pmatrix}. \quad (\text{B2})$$

Then

$$\|B\|_1 \leq \sqrt{W} \left\| \sqrt{A^g} B \sqrt{D^g} \right\|_\infty, \quad (\text{B3})$$

where $(\cdot)^g$ denotes the generalized inverse, and $W = \text{Tr}[\rho^\Pi]$ as defined above.

Proof.—First, we briefly prove the standard result $\Pi A \Pi \geq 0$ for any $A \geq 0$ and projection Π . Equivalently, we show that $\langle v | \Pi A \Pi | v \rangle \geq 0 \forall v$. Let $|w\rangle = \Pi |v\rangle$. Thus, $\langle v | \Pi A \Pi | v \rangle = \langle w | A | w \rangle \geq 0$ showing that

$$\Pi A \Pi \geq 0. \quad (\text{B4})$$

In particular, this implies that $\rho^\Pi \geq 0$. Since the 1-norm of a positive semidefinite operator is its trace,

$$\|\rho^\Pi\|_1 = \text{Tr}[\rho^\Pi] = W. \quad (\text{B5})$$

Define

$$\rho_\lambda = \begin{pmatrix} A & \frac{1}{\lambda}B \\ \frac{1}{\lambda}B^\dagger & D \end{pmatrix},$$

where $\lambda = \left\| \sqrt{A^g} B \sqrt{D^g} \right\|_\infty$. We have defined ρ_λ such that $\text{Tr} \left[\rho_\lambda^{\Pi} \right] = W$. Using Theorem IX.5.9 from Ref. [37] gives us that $\rho_\lambda \geq 0$. Thus, we can apply the observation of Eq. (B1) on ρ_λ to get

$$\left\| \frac{1}{\lambda} B \right\|_1 \leq \sqrt{W} \quad (\text{B6})$$

$$\implies \|B\|_1 \leq \lambda \sqrt{W}, \quad (\text{B7})$$

which completes the proof. \blacksquare

Corollary 9.1.—Define $H = \begin{pmatrix} 0 & B \\ B^\dagger & 0 \end{pmatrix}$ as the block off-diagonal part of ρ . Then $\|H\|_1 \leq 2\sqrt{W} \left\| \sqrt{A^g} B \sqrt{D^g} \right\|_\infty$.

Proof.—

$$\|H\|_1 = \text{Tr} \left[\sqrt{H^\dagger H} \right] \quad (\text{B8})$$

$$= \text{Tr} \left[\begin{pmatrix} \sqrt{BB^\dagger} & 0 \\ 0 & \sqrt{B^\dagger B} \end{pmatrix} \right] \quad (\text{B9})$$

$$= 2 \|B\|_1 \quad (\text{B10})$$

$$\leq 2\lambda \sqrt{W}, \quad (\text{B11})$$

where $\lambda = \left\| \sqrt{A^g} B \sqrt{D^g} \right\|_\infty$ as defined in Theorem 9. \blacksquare

2. Bounds on expectation values

Let $\text{Tr} \left[P^\Pi \right] \leq W$. Given a POVM element Γ , the proofs of Lemma 2 and Lemma 3 require upper and lower bounds of the form $\text{Tr} \left[A^\Pi \Gamma \right]$. We derive these bounds in this Appendix.

First note that $\|H\|_1 \leq 2\lambda \sqrt{W}$ as shown in Eq. (B11). As H is Hermitian, $H = H_+ - H_-$ for some $H_+, H_- \geq 0$. Since H is traceless, $\text{Tr} [H_+] = \text{Tr} [H_-]$. Thus,

$$\|H\|_1 = \text{Tr} [H_+] + \text{Tr} [H_-] \quad (\text{B12})$$

$$= 2\text{Tr} [H_+] \quad (\text{B13})$$

$$= 2\text{Tr} [H_-]. \quad (\text{B14})$$

We can then calculate the upper bound

$$\text{Tr} [A^\Pi \Gamma] = \text{Tr} [A\Gamma] - \text{Tr} [A^\Pi \Gamma] - \text{Tr} [H_+ \Gamma] + \text{Tr} [H_- \Gamma] \quad (\text{B15})$$

$$\leq \text{Tr} [A\Gamma] + \text{Tr} [H_-] \quad (\text{B16})$$

$$= \text{Tr} [A\Gamma] + \lambda \sqrt{W}, \quad (\text{B17})$$

where the inequality follows from matrix Hölder's inequality $\text{Tr} [H_- \Gamma] \leq \|\Gamma\|_\infty \|H_-\|_1$, and noting that $A^\Pi \geq 0$ as shown in Eq. (B4). Similarly, we can compute the lower bound

$$\text{Tr} [A^\Pi \Gamma] = \text{Tr} [A\Gamma] - \text{Tr} [A^\Pi \Gamma] - \text{Tr} [H_+ \Gamma] + \text{Tr} [H_- \Gamma] \quad (\text{B18})$$

$$\geq \text{Tr} [A\Gamma] - \text{Tr} [A^\Pi \Gamma] - \text{Tr} [H_-] \quad (\text{B19})$$

$$= \text{Tr} [A\Gamma] - W - \lambda \sqrt{W}. \quad (\text{B20})$$

3. Proof of Lemma 2

Here we prove Lemma 2 from the main text.

Lemma 2.—Define

$$E_M := \{J^M \in \mathcal{B}(\mathcal{H}_M \otimes \mathcal{K}) \mid \text{Tr}_{\mathcal{K}} [J^M] \leq \Pi_M,$$

$$J^M \geq 0, \text{Tr} \left[(\rho_k^{\mu T} \otimes \Gamma_l) J^M \right] \leq \gamma_{l|k,\mu} + \epsilon_{kM}^\mu,$$

$$\text{Tr} \left[(\rho_k^{\mu T} \otimes \Gamma_l) J^M \right] \geq \gamma_{l|k,\mu} - w_{kM}^\mu - \epsilon_{kM}^\mu \quad \forall k, l, \mu \}. \quad (\text{B21})$$

Then, $(\Pi_M \otimes \mathbb{I}_{\mathcal{K}}) S_\infty (\Pi_M \otimes \mathbb{I}_{\mathcal{K}}) \subseteq E_M$ where S_∞ is as defined in Eq. (15).

Proof.—Consider any $J \in S_\infty$ where $\text{Tr} \left[(\rho_k^{\mu T} \otimes \Gamma_l) J \right] = \gamma_{l|k,\mu}$. From Eq. (23) we get that $(\Pi_M \otimes \mathbb{I}_{\mathcal{K}}) J (\Pi_M \otimes \mathbb{I}_{\mathcal{K}}) \geq 0$, and Lemma 1 implies that $\text{Tr}_{\mathcal{K}} [(\Pi_M \otimes \mathbb{I}_{\mathcal{K}}) J (\Pi_M \otimes \mathbb{I}_{\mathcal{K}})] \leq \Pi_M$.

We now show that $(\Pi_M \otimes \mathbb{I}_{\mathcal{K}}) J (\Pi_M \otimes \mathbb{I}_{\mathcal{K}}) \in E_M$ by bounding its expectation values. First, note that

$$\text{Tr} \left[(\rho_k^{\mu T} \otimes \Gamma_l) (\Pi_M \otimes \mathbb{I}_{\mathcal{K}}) J (\Pi_M \otimes \mathbb{I}_{\mathcal{K}}) \right] = \text{Tr} \left[(\rho_k^{\mu M T} \otimes \Gamma_l) J \right] \quad (\text{B21})$$

$$= \text{Tr} \left[\Gamma_l \Phi(\rho_k^{\mu M T}) \right] \quad (\text{B22})$$

$$= \text{Tr} \left[\Phi^\dagger(\Gamma_l) \rho_k^{\mu M T} \right], \quad (\text{B23})$$

where we have used the cyclic property of trace to get Eq. (B21), and the fact that $J \in S_\infty$ is the Choi isomorphism of a channel Φ to get Eq. (B22).

Note that for any POVM element $\Gamma_l \leq \mathbb{I}_{\mathcal{K}}$, it is the case that $\Phi^\dagger(\Gamma_l) \leq \mathbb{I}_{\mathcal{H}}$ is also a POVM element on \mathcal{H} . This implies that $\|\Phi^\dagger(\Gamma_l)\|_\infty \leq 1$. Thus, we can use the results proved in Appendix B2 as follows.

Lower bound:

$$\text{Tr} \left[\Phi^\dagger(\Gamma_l) \rho_k^{\mu M T} \right] \geq \text{Tr} \left[\Phi^\dagger(\Gamma_l) \rho_k^{\mu T} \right] - w_{kM}^\mu - \frac{\|H_k^{\mu M}\|_1}{2} \quad (\text{B24})$$

$$= \gamma_{l|k,\mu} - w_{kM}^\mu - \frac{\|H_k^{\mu M}\|_1}{2} \quad (\text{B25})$$

$$\geq \gamma_{l|k,\mu} - w_{kM}^\mu - \epsilon_{kM}^\mu \quad (\text{B26})$$

Upper bound:

$$\text{Tr} \left[\Phi^\dagger(\Gamma_l) \rho_k^{\mu M T} \right] \leq \text{Tr} \left[\Phi^\dagger(\Gamma_l) \rho_k^{\mu T} \right] + \frac{\|H_k^{\mu M}\|_1}{2} \quad (\text{B27})$$

$$= \gamma_{l|k,\mu} + \frac{\|H_k^{\mu M}\|_1}{2} \quad (\text{B28})$$

$$\leq \gamma_{l|k,\mu} + \epsilon_{kM}^\mu, \quad (\text{B29})$$

where Eqs. (B25) and (B28) follow from the expectation value constraint on $J \in \mathcal{S}_\infty$, and Eqs. (B26) and (B29) follow from the fact that $\|H_k^{\mu M}\|_1 \leq 2\epsilon_{kM}^\mu$ proved in Appendix B 1. Thus, we have shown that $(\Pi_M \otimes \mathbb{I}_{\mathcal{K}})J(\Pi_M \otimes \mathbb{I}_{\mathcal{K}}) \in E_M$ for all $J \in \mathcal{S}_\infty$ completing the proof. ■

4. Proof of Lemma 3

Lemma 3.—Let $[\Pi_N, \Gamma_l] = 0 \forall l$, and define

$$\begin{aligned} S_{MN} := & \{J^{MN} \in \mathcal{B}(\mathcal{H}_M \otimes \mathcal{K}_N) \mid \\ & \text{Tr}_{\mathcal{K}} [J^{MN}] \leq \Pi_M, J^{MN} \geq 0, \\ & \text{Tr} \left[(\rho_k^{\mu T} \otimes \Gamma_l) J^{MN} \right] \geq \gamma_{l|k,\mu} - W_{kN}^\mu - w_{kM}^\mu - 2\epsilon_{kM}^\mu, \\ & \text{Tr} \left[(\rho_k^{\mu T} \otimes \Gamma_l) J^{MN} \right] \leq \gamma_{l|k,\mu} + \epsilon_{kM}^\mu \forall k, l, \mu \}. \end{aligned} \quad (\text{28})$$

Then, $(\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) E_M (\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) \subseteq S_{MN}$ where E_M is as defined in Eq. (26).

Proof.—Consider some $J^M \in E_M$. We observe that $(\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) J^M (\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) \geq 0$ from Eq. (23) and $\text{Tr}_{\mathcal{K}} [(\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) J^M (\mathbb{I}_{\mathcal{H}} \otimes \Pi_N)] \leq \Pi_M$ from Lemma 1. Next we prove that $(\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) J^M (\mathbb{I}_{\mathcal{H}} \otimes \Pi_N)$ satisfies the lower bound of the expectation value constraint described in Eq. (28).

First, we state some preliminary results. Using Lemma 2 with Eq. (27), we show that

$$\text{Tr} \left[(\rho_k^{\mu T} \otimes \Pi_N) J^M \right] \geq 1 - W_{kN}^\mu - w_{kM}^\mu - \epsilon_{kM}^\mu. \quad (\text{B30})$$

Since $[\Pi_N, \Gamma_l] = 0$, we can write

$$\Gamma_l = \Gamma_l^N + \Gamma_l^{\bar{N}}, \quad (\text{B31})$$

where $\Gamma_l^{\bar{N}} := \bar{\Pi}_N \Gamma_l \bar{\Pi}_N$. We can also show that

$$\text{Tr} \left[(\rho_k^{\mu M T} \otimes \mathbb{I}_{\mathcal{K}}) J^M \right] = \text{Tr} \left[\rho_k^{\mu M T} \text{Tr}_{\mathcal{K}} [J^M] \right] \quad (\text{B32})$$

$$\leq \text{Tr} \left[\rho_k^{\mu M T} \Pi_M \right] \quad (\text{B33})$$

$$= \text{Tr} \left[\rho_k^{\mu M T} \right] \quad (\text{B34})$$

$$= 1 - w_{kM}^\mu, \quad (\text{B35})$$

where the inequality follows from the definition of E_M in Lemma 2. Additionally, note that

$$\text{Tr} \left[(\rho_k^{\mu T} \otimes \Gamma_l) J^M \right] = \text{Tr} \left[(\rho_k^{\mu M T} \otimes \Gamma_l) J^M \right] \quad (\text{B36})$$

since $J^M \in \mathcal{B}(\mathcal{H}_M \otimes \mathcal{K})$.

We can use this to estimate the lower bound as shown below.

$$\begin{aligned} & \text{Tr} \left[(\rho_k^{\mu T} \otimes \Gamma_l) (\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) J^M (\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) \right] \\ &= \text{Tr} \left[(\rho_k^{\mu T} \otimes \Gamma_l) J^M \right] - \text{Tr} \left[(\rho_k^{\mu M T} \otimes \Gamma_l) J^M \right] \\ & \quad + \text{Tr} \left[(\rho_k^{\mu M T} \otimes \Gamma_l^N) J^M \right] \end{aligned} \quad (\text{B37})$$

$$= \text{Tr} \left[(\rho_k^{\mu T} \otimes \Gamma_l) J^M \right] - \text{Tr} \left[(\rho_k^{\mu M T} \otimes \Gamma_l^{\bar{N}}) J^M \right] \quad (\text{B38})$$

$$\geq \text{Tr} \left[(\rho_k^{\mu T} \otimes \Gamma_l) J^M \right] - \text{Tr} \left[(\rho_k^{\mu M T} \otimes \bar{\Pi}_N) J^M \right] \quad (\text{B39})$$

$$\begin{aligned} &= \text{Tr} \left[(\rho_k^{\mu T} \otimes \Gamma_l) J^M \right] - \text{Tr} \left[(\rho_k^{\mu M T} \otimes \mathbb{I}_{\mathcal{K}}) J^M \right] \\ & \quad + \text{Tr} \left[(\rho_k^{\mu M T} \otimes \Pi_N) J^M \right] \end{aligned} \quad (\text{B40})$$

$$\begin{aligned} &\geq \text{Tr} \left[(\rho_k^{\mu T} \otimes \Gamma_l) J^M \right] - (1 - w_{kM}^\mu) \\ & \quad + (1 - W_{kN}^\mu - w_{kM}^\mu - \epsilon_{kM}^\mu) \end{aligned} \quad (\text{B41})$$

$$\geq \gamma_{l|k,\mu} - w_{kM}^\mu - 2\epsilon_{kM}^\mu - W_{kN}^\mu, \quad (\text{B42})$$

where Eq. (B37) follows from Eqs. (B36) and (B38) follows from Eqs. (B31), (B39) follows from the fact that $\Gamma_l \leq \mathbb{I}_{\mathcal{K}}$, Eq. (B41) follows from Eqs. (B30), (B35), and (B42) follows from the fact that $J^M \in E_M$.

Finally, the fact that the projector commutes with the measurements $[\Pi_N, \Gamma_l] = 0$ immediately gives the upper

bound

$$\text{Tr} \left[\left(\rho_k^{\mu T} \otimes \Gamma_l^N \right) J^M \right] \leq \text{Tr} \left[\left(\rho_k^{\mu T} \otimes \Gamma_l \right) J^M \right] \quad (\text{B43})$$

$$\leq \gamma_{l|k,\mu} + \epsilon_{kM}^{\mu} \quad (\text{B44})$$

since $\left(\rho_k^{\mu T} \otimes \Gamma_l \right) - \left(\rho_k^{\mu T} \otimes \Gamma_l^N \right) \geq 0$. Thus, we have shown that for all $J^M \in \text{EV}_M$, $(\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) J^M (\mathbb{I}_{\mathcal{H}} \otimes \Pi_N) \in \text{S}_{MN}$ completing the proof. ■

5. Closeness of eigenvectors

As in this paper, one might run into a situation where diagonalizing a density matrix ρ is of interest, while a perturbed density matrix $\sigma = \rho + H$ can be diagonalized where $\|H\|_1 \leq 2\epsilon$. In this Appendix, we explain how and when one can approximate the eigenvectors of ρ with the eigenvectors of σ .

Let $\lambda_i(S)$ be the i th largest eigenvalue of a compact, self-adjoint operator S . From Theorem 4.10 of Ref. [44], we can write the eigenvalues as

$$\lambda_n(S) = \min_{\{|\psi_1\rangle, \dots, |\psi_{n-1}\rangle\}} \max_{|\psi\rangle \in P^\perp(\{|\psi_1\rangle, \dots, |\psi_{n-1}\rangle\})} \langle \psi | S | \psi \rangle,$$

where $P^\perp(\{|\psi_1\rangle, \dots, |\psi_{n-1}\rangle\}) := \{|\psi\rangle \in \text{span}\{|\psi_1\rangle, \dots, |\psi_{n-1}\rangle\}^\perp \mid \|\psi\| = 1\}$ is the space perpendicular to the vectors $|\psi_1\rangle, \dots, |\psi_{n-1}\rangle$. From this we can bound the change in eigenvalues due to the perturbation.

Theorem 10.—Let \mathcal{H} be a Hilbert space. Given $\rho \in \text{D}(\mathcal{H})$, $\sigma \in \text{D}(\mathcal{H})$ and $H = \sigma - \rho$ with $\|H\|_1 \leq 2\epsilon$ as defined above,

$$|\lambda_i(\rho) - \lambda_i(\sigma)| \leq \epsilon$$

for all eigenvalues indexed by i .

Proof.—The proof follows similarly to the proof of Weyl's inequality, which is for finite dimensions.

$$\begin{aligned} \lambda_i(\sigma) &= \min_{\{|\psi_1\rangle, \dots, |\psi_{i-1}\rangle\}} \max_{|\psi\rangle \in P^\perp(\{|\psi_1\rangle, \dots, |\psi_{i-1}\rangle\})} \\ &\quad \times \langle \psi | S | \psi \rangle \langle \psi | \sigma | \psi \rangle \\ &= \min_{\{|\psi_1\rangle, \dots, |\psi_{i-1}\rangle\}} \max_{|\psi\rangle \in P^\perp(\{|\psi_1\rangle, \dots, |\psi_{i-1}\rangle\})} \\ &\quad \times (\langle \psi | \rho | \psi \rangle + \langle \psi | H | \psi \rangle) \\ &\leq \min_{\{|\psi_1\rangle, \dots, |\psi_{i-1}\rangle\}} \\ &\quad \times \left(\max_{|\psi\rangle \in P^\perp(\{|\psi_1\rangle, \dots, |\psi_{i-1}\rangle\})} \langle \psi | \rho | \psi \rangle + \|H\|_\infty \right) \\ &= \lambda_i(\rho) + \|H\|_\infty \\ &\leq \lambda_i(\rho) + \frac{\|H\|_1}{2} \end{aligned} \quad (\text{B45})$$

$$= \lambda_i(\rho) + \epsilon, \quad (\text{B46})$$

where Eq. (B45) follows from noting that $\text{Tr}[H] = 0$. Starting with ρ instead of σ in the first line and following the same steps while replacing H with $-H$ gives us $\lambda_i(\rho) \leq \lambda_i(\sigma) + \epsilon$. Combining both together, we get $|\lambda_i(\rho) - \lambda_i(\sigma)| \leq \epsilon$ as stated. ■

Before talking about the individual eigenvectors, we shall introduce the Davis-Kahan theorem [45]. The intuition of the theorem can be understood as follows. Any density operator can be diagonalized as

$$\tau = W_\tau D_\tau W_\tau^\dagger,$$

where W_τ is a unitary whose columns are the eigenvectors of τ , and D_τ is a diagonal operator whose elements are eigenvalues of τ . The unitary can be written as a block matrix

$$W_\tau = [W \quad W_\perp],$$

where W and W_\perp are isometries whose columns span eigenspaces of τ . If τ is not degenerate, these eigenspaces are orthogonal to each other. The density operator τ can be written as

$$\tau = W\tau_0 W^\dagger + W_\perp \tau_1 W_\perp^\dagger,$$

where τ_0 and τ_1 are diagonal matrices whose elements are the eigenvalues of τ corresponding to the eigenvectors in W and W_\perp , respectively.

Let ρ and σ have decompositions with $U_\rho = [U \quad U_\perp]$ and $V_\sigma = [V \quad V_\perp]$. The theorem then formalizes the intuition that if ρ and σ are ‘‘close’’, then the eigenspaces spanned by U and V_\perp are ‘‘almost’’ orthogonal.

Theorem 11 (Davis-Kahan).—Let $\rho = U\rho_0 U^\dagger + U_\perp \rho_1 U_\perp^\dagger$ and $\sigma = V\sigma_0 V^\dagger + V_\perp \sigma_1 V_\perp^\dagger$ be density operators where the block matrices $[U \quad U_\perp]$ and $[V \quad V_\perp]$ are unitaries. Let $H = \sigma - \rho$. If the eigenvalues of ρ_0 are contained in an interval (a, b) , and the eigenvalues of σ_1 are excluded from the interval $(a - \delta, b + \delta)$ for some $\delta > 0$, then

$$\left\| V_\perp^\dagger U \right\| \leq \frac{\left\| V_\perp^\dagger H U \right\|}{\delta} \quad (\text{B47})$$

for any unitarily invariant norm $\|\cdot\|$.

Although the proof in Ref. [45] is for finite dimensions, the proof for infinite-dimensional density operators is exactly the same. Intuitively, the δ represents how separated the eigenspaces of σ are relative to the perturbation ϵ . If this δ is too small, the corresponding eigenspaces of ρ and σ could be quite different. Instructive examples and further intuition about this theorem can be found in Ref. [45].

Corollary 11.1.—Let ρ, σ be density operators with $H = \sigma - \rho$ and $\|H\|_1 \leq 2\epsilon$. Define $\delta_i = \min\{\lambda_i(\sigma) - \lambda_{i-1}(\sigma) - \epsilon, \lambda_{i+1}(\sigma) - \lambda_i(\sigma) - \epsilon\}$. Then

$$F(U_i U_i^\dagger, V_i V_i^\dagger) \geq 1 - \frac{\epsilon^2}{\delta_i^2}, \quad (\text{B48})$$

where U_i and V_i are the i th eigenvectors of ρ and σ , respectively.

Proof.—For each i , let ρ and σ have decomposition

$$\rho = U_i \lambda_i(\rho) U_i^\dagger + U_{i\perp} \rho_1 U_{i\perp}^\dagger \quad (\text{B49})$$

$$\sigma = V_i \lambda_i(\sigma) V_i^\dagger + V_{i\perp} \sigma_1 V_{i\perp}^\dagger \quad (\text{B50})$$

as described in Theorem 11. A direct consequence of Theorem 10 is that $\lambda_i(\rho)$ lies in the interval (a_i, b_i) with $a_i = \lambda_i(\sigma) - \epsilon$ and $b_i = \lambda_i(\sigma) + \epsilon$. Additionally, it can be easily verified that all the eigenvalues of σ_1 lie outside the interval $(a_i - \delta_i, b_i + \delta_i)$. Thus, using Theorem 11

$$\|V_{i\perp}^\dagger U_i\|_\infty \leq \frac{\|V_{i\perp}^\dagger H U_i\|_\infty}{\delta_i} \quad (\text{B51})$$

$$\leq \frac{\|V_{i\perp}^\dagger\|_\infty \|H\|_\infty \|U_i\|_\infty}{\delta_i} \quad (\text{B52})$$

$$= \frac{\|H\|_\infty}{\delta_i} \quad (\text{B53})$$

$$\leq \frac{\|H\|_1}{2\delta_i} \quad (\text{B54})$$

$$\leq \frac{\epsilon}{\delta_i}, \quad (\text{B55})$$

where the second inequality follows from the fact that the ∞ norm is submultiplicative $\|AB\|_\infty \leq \|A\|_\infty \|B\|_\infty$, and the succeeding equality is a consequence of the fact that $\|W\|_\infty = 1$ for any isometry W .

Now consider the diagonalizing unitaries $U_\rho = [U_i \ U_{i\perp}]$ and $V_\sigma = [V_i \ V_{i\perp}]$. Thus,

$$W := U_\rho^\dagger V_\sigma = \begin{pmatrix} U_i^\dagger V_i & U_i^\dagger V_{i\perp} \\ U_{i\perp}^\dagger V_i & U_{i\perp}^\dagger V_{i\perp} \end{pmatrix}$$

must also be unitary. So $WW^\dagger = \mathbb{I}$. Looking at the first block of WW^\dagger , which is one dimensional,

$$U_i^\dagger V_i V_i^\dagger U_i + U_i^\dagger V_{i\perp} V_{i\perp}^\dagger U_i = 1. \quad (\text{B56})$$

Thus,

$$\left| 1 - U_i^\dagger V_i V_i^\dagger U_i \right| = \left\| 1 - U_i^\dagger V_i V_i^\dagger U_i \right\|_\infty \quad (\text{B57})$$

$$= \left\| U_i^\dagger V_{i\perp} V_{i\perp}^\dagger U_i \right\|_\infty \quad (\text{B58})$$

$$\leq \left\| U_i^\dagger V_{i\perp} \right\|_\infty \left\| V_{i\perp}^\dagger U_i \right\|_\infty \quad (\text{B59})$$

$$\leq \frac{\epsilon^2}{\delta_i^2}, \quad (\text{B60})$$

where Eq. (B60) follows from Eq. (B55). Observe that the fidelity between the eigenvectors U_i and V_i is $\left| U_i^\dagger V_i \right|$. Equation (B60) then directly gives us a bound on the fidelity,

$$F(U_i U_i^\dagger, V_i V_i^\dagger)^2 \geq 1 - \frac{\epsilon^2}{\delta_i^2}. \quad (\text{B61})$$

Theorem 6 from the main text is just a special case of Theorem 10, and Corollary 11.1 as follows. Let $\sigma = \rho^\Pi + \rho^{\bar{\Pi}}$ and $H = \sigma - \rho$. Corollary 9.1 gives $\|H\|_1 \leq 2 \left\| \sqrt{\rho^{\Pi^g}} \Pi \rho \bar{\Pi} \sqrt{\rho^{\bar{\Pi}^g}} \right\|_\infty \sqrt{\text{Tr}[\rho^{\bar{\Pi}}]}$. Thus, defining $\epsilon_{\text{proj}} = \left\| \sqrt{\rho^{\Pi^g}} \Pi \rho \bar{\Pi} \sqrt{\rho^{\bar{\Pi}^g}} \right\|_\infty \sqrt{\text{Tr}[\rho^{\bar{\Pi}}]}$, Theorem 6 is exactly Theorem 10 and Corollary 11.1. ■

As a final remark, we note that all the results in this Appendix hold if we replace ϵ with ϵ_∞ , where $\|H\|_\infty \leq \epsilon_\infty$.

APPENDIX C: BOUND ON WEIGHT OUTSIDE PROJECTED SUBSPACE

The general method of using ‘‘cross-clicks’’ to bound the weight outside the projected subspace is taken from Chap. 2 of Ref. [46].

Since we use threshold detectors, Bob’s measurements are block diagonal in the total photon number of the two pulses. Given the probability that Bob received a state with n photons $p(n)$, the probability $p(\text{event})$ of observing a particular detection event can then be written as

$$p(\text{event}) = \sum_{n=0}^{\infty} p(n) p(\text{event} | n), \quad (\text{C1})$$

$$= \sum_{n=0}^N p(n) p(\text{event} | n) + \sum_{n=N+1}^{\infty} p(n) p(\text{event} | n), \quad (\text{C2})$$

$$\geq p(\leq N) p^{\min}(\text{event} | \leq N) + p(> N) p^{\min}(\text{event} | > N), \quad (\text{C3})$$

where $p^{\min}(\text{event} | \leq N)$ denotes the minimum probability of observing the detection event given the state has

$\leq N$ photons. Using the fact that $p(\leq N) + p(> N) = 1$ and rearranging we get

$$p(>N) \leq \frac{p(\text{event}) - p^{\min}(\text{event} \mid \leq N)}{p^{\min}(\text{event} \mid > N) - p^{\min}(\text{event} \mid \leq N)}. \quad (\text{C4})$$

So in order to bound the weight outside the $\leq N$ subspace, we need to find $p(\text{event} \mid n)$.

We have some choice when choosing the specific event, which we call a ‘‘cross-click’’ event. Here, we define a cross-click to be any click pattern that records a click in both the detectors while ignoring all clicks in mode d_2 , which corresponds to the missing detector. We make this choice because it makes the calculations simpler as shall become apparent. We do not claim that this is the optimal choice. However, as shown above, the validity of the bounds in Eq. (C4) are independent of the choice of detection event.

We wish to bound the probability $p(cc \mid n)$ of cross-clicks over all input states with n total photons in both pulses. Although this task is hard for a generic choice of cross-click event, our specific choice allows us to simplify the task with the following observation. The probability of cross-clicks $p(cc)$ does not depend on either the phase or the relative phase of the two pulses. Thus, without loss of generality, we can always consider individually phase-randomized pulses without changing the statistics. In other words, we can assume that our input state is a probabilistic mixture of $|m, n - m\rangle \langle m, n - m|$ where the total photon number is n . Thus, it is sufficient to bound the probability $p(cc \mid n)$ of cross-clicks over all input states with m photons in the first pulse, and $n - m$ photons in the second.

We consider the generic case where Bob’s passive basis choice beam splitter has ratio $(1 - t)/t$. This can be used to obtain the results for Sec. VI by setting $t = 0.1$. As shown in Fig. 7, the probability of a cross-click given an input state containing m and $n - m$ photons in the two pulses is

$$\begin{aligned} p(cc \mid m, n - m) &= \sum_{\substack{a+b \neq 0 \\ a+b \neq n}} \binom{m}{b} \binom{n-m}{a} t^{a+b} (1-t)^{n-a-b} \\ &\quad \times \left(\frac{1}{2}\right)^{a+b} \sum_{c+d \neq 0} \binom{a}{c} \binom{b}{d} \left(1 - \left(\frac{1}{2}\right)^{c+d}\right). \end{aligned} \quad (\text{C5})$$

Here, $\binom{m}{b} t^b (1-t)^{m-b}$ factor reflects the probability of m input photons being split into $m - b$ and b photons. The $\binom{b}{d} (1/2)^b$ factor reflects the probability of b photons being split into d and $b - d$ photons for the two arms of the interferometer. Similarly, the same reasoning applies for the input pulse with $n - d$ photons. The last $(1 - (1/2)^{c+d})$

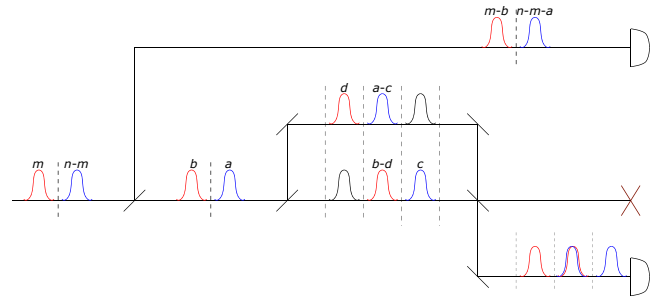


FIG. 7. Bob receives m and $n - m$ photons in the two pulses. Of that $a + b$ photons go into the X -basis measurement line, and $n - a - b$ go to the Z -basis detector. c and d photons go into the outside time bins of the interferometer with the rest going into the middle time bin.

factor is to subtract the case when all $c + d$ photons go into the line with the detector we do not use.

We first calculate the second summation,

$$S(a, b) = \sum_{c+d \neq 0} \binom{a}{c} \binom{b}{d} \left(1 - \left(\frac{1}{2}\right)^{c+d}\right) \quad (\text{C6})$$

$$= \sum_{c=0}^a \sum_{d=0}^b \binom{a}{c} \binom{b}{d} \left(1 - \left(\frac{1}{2}\right)^{c+d}\right) - 0 \quad (\text{C7})$$

$$= 2^{a+b} - \left(\frac{3}{2}\right)^{a+b}. \quad (\text{C8})$$

Thus, the cross-click probability can be simplified as

$$\begin{aligned} p(cc \mid m, n - m) &= \sum_{\substack{a+b \neq 0 \\ a+b \neq n}} \binom{m}{b} \binom{n-m}{a} t^{a+b} (1-t)^{n-a-b} \left(\frac{1}{2}\right)^{a+b} S(a, b) \\ &= \sum_{\substack{a+b \neq 0 \\ a+b \neq n}} \binom{m}{b} \left(\frac{t}{2}\right)^b (1-t)^{m-b} \binom{n-m}{a} \\ &\quad \times \left(\frac{t}{2}\right)^a (1-t)^{n-m-a} S(a, b). \end{aligned} \quad (\text{C9})$$

$$\begin{aligned} &= \sum_{\substack{a+b \neq 0 \\ a+b \neq n}} \binom{m}{b} \left(\frac{t}{2}\right)^b (1-t)^{m-b} \binom{n-m}{a} \\ &\quad \times \left(\frac{t}{2}\right)^a (1-t)^{n-m-a} S(a, b). \end{aligned} \quad (\text{C10})$$

In order to simplify this, we compute

$$f(x, m) = \sum_{b=0}^m \binom{m}{b} \left(\frac{t}{2}\right)^b (1-t)^{m-b} x^b \quad (\text{C11})$$

$$= \left(1 - t + \frac{xt}{2}\right)^m. \quad (\text{C12})$$

So using Eq. (C12) in Eq. (C10) we get

$$\begin{aligned}
 p(\text{cc} | m, n - m) &= f(2, m)f(2, n - m) \\
 &\quad - f\left(\frac{3}{2}, m\right)f\left(\frac{3}{2}, n - m\right) \\
 &\quad - \left(\frac{2t}{2}\right)^n + \left(\frac{3t}{4}\right)^n \quad (\text{C13})
 \end{aligned}$$

$$\begin{aligned}
 &= \left(1 - t + \frac{2t}{2}\right)^n - \left(1 - t + \frac{3t}{4}\right)^n \\
 &\quad - t^n + \left(\frac{3t}{4}\right)^n \quad (\text{C14})
 \end{aligned}$$

$$= 1 - t^n - \left(1 - \frac{t}{4}\right)^n + \left(\frac{3t}{4}\right)^n. \quad (\text{C15})$$

We observe that the cross-click probability does not depend on m , which intuitively follows from the symmetry of our definition of cross-clicks.

Viewing the cross-click probability as a function of n

$$f(n) = 1 - t^n - \left(1 - \frac{t}{4}\right)^n + \left(\frac{3t}{4}\right)^n, \quad (\text{C16})$$

we look to show that the function is monotonically increasing. This would make it easy to find $p^{\min}(\text{cc} | \leq N)$. We do this by considering

$$\begin{aligned}
 f(n + 1) - f(n) &= t^n(1 - t) + \left(1 - \frac{t}{4}\right)^n \left(\frac{t}{4}\right) \\
 &\quad - \left(\frac{3t}{4}\right)^n \left(1 - \frac{3t}{4}\right) \quad (\text{C17})
 \end{aligned}$$

and showing that this is positive for all positive integers n . We first note that $0 \leq t \leq 1$, which gives us

$$t \leq 1, \quad (\text{C18})$$

$$1 - t \geq 0, \quad (\text{C19})$$

$$1 - \frac{t}{4} - \frac{3t}{4} \geq 0, \quad (\text{C20})$$

$$1 - \frac{t}{4} \geq \frac{3t}{4}. \quad (\text{C21})$$

Raising both sides to the n th power and multiplying both sides of the inequality by $t/4$,

$$\left(1 - \frac{t}{4}\right)^n \frac{t}{4} \geq \left(\frac{3t}{4}\right)^n \frac{t}{4} \quad (\text{C22})$$

$$\left(1 - \frac{t}{4}\right)^n \frac{t}{4} - \left(\frac{3t}{4}\right)^n \left(1 - \frac{3t}{4}\right) \geq \left(\frac{3t}{4}\right)^n (t - 1). \quad (\text{C23})$$

Finally, adding $t^n(1 - t)$ to both sides of the equation,

$$\begin{aligned}
 t^n(1 - t) + \left(1 - \frac{t}{4}\right)^n \frac{t}{4} - \left(\frac{3t}{4}\right)^n \left(1 - \frac{3t}{4}\right) \\
 \geq t^n(1 - t) + \left(\frac{3t}{4}\right)^n (t - 1), \quad (\text{C24})
 \end{aligned}$$

$$f(n + 1) - f(n) \geq \left(t^n - \left(\frac{3t}{4}\right)^n\right)(1 - t) \geq 0, \quad (\text{C25})$$

where the last inequality follows from the fact that $t \geq 3t/4$. Thus, $p^{\min}(\text{cc} | \leq N) = p(\text{cc} | 0) = 0$, and $p^{\min}(\text{cc} | > N) = p(\text{cc} | N + 1)$. Using this in Eq. (C4),

$$p(>N) \leq \frac{p(\text{cc})}{1 - t^{N+1} - \left(1 - \frac{t}{4}\right)^{N+1} + \left(\frac{3t}{4}\right)^{N+1}}, \quad (\text{C26})$$

where we can obtain the cross-click probability $p(\text{cc})$ from the observations.

-
- [1] Michele Mosca, Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Secur. Priv.* **16**, 38 (2018).
 - [2] Dominic Mayers, in *Annual International Cryptology Conference* (Springer, 1996), p. 343.
 - [3] Dominic Mayers, Unconditional security in quantum cryptography, *J. ACM* **48**, 351 (2001).
 - [4] Renato Renner, Nicolas Gisin, and Barbara Kraus, Information-theoretic security proof for quantum-key-distribution protocols, *Phys. Rev. A* **72**, 012332 (2005).
 - [5] Marco Lucamarini, Andrew Shields, Romain Alléaume, Christopher Chunnillall, Ivo Pietro Degiovanni, Marco Gramegna, Atilla Hasekioglu, Bruno Huttner, Rupesh Kumar, Andrew Lord, *et al.*, Implementation security of quantum cryptography—introduction, challenges, solutions—ETSI white paper no. 27. 2018.
 - [6] Margarida Pereira, Marcos Curty, and Kiyoshi Tamaki, Quantum key distribution with flawed and leaky sources, *Npj Quantum Inf.* **5**, 1 (2019).
 - [7] Margarida Pereira, Go Kato, Akihiro Mizutani, Marcos Curty, and Kiyoshi Tamaki, Quantum key distribution with correlated sources, *Sci. Adv.* **6**, eaaz4487 (2020).
 - [8] Practical quantum key distribution that is secure against side channels, *Phys. Rev. Appl.* **15**, 034072 (2021).
 - [9] Won-Young Hwang, Quantum key distribution with high loss: Toward global secure communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
 - [10] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, Decoy state quantum key distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
 - [11] Xiang-Bin Wang, Beating the photon-number-splitting attack in practical quantum cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).
 - [12] Security of quantum key distribution with intensity correlations, *Quantum* **5**, 602 (2021).

- [13] Xoel Sixto, Víctor Zapatero, and Marcos Curty, Security of decoy-state quantum key distribution with correlated intensity fluctuations, *Phys. Rev. Appl.* **18**, 044069 (2022).
- [14] Toshiya Kobayashi, Akihisa Tomita, and Atsushi Okamoto, Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser, *Phys. Rev. A* **90**, 032320 (2014).
- [15] Guillermo Currás-Lorenzo, Shlok Nahar, Norbert Lütkenhaus, Kiyoshi Tamaki, and Marcos Curty, Security of quantum key distribution with imperfect phase randomisation, *Quantum Sci. Technol.* (2023).
- [16] Shi-Hai Sun, Feihu Xu, Mu-Sheng Jiang, Xiang-Chun Ma, Hoi-Kwong Lo, and Lin-Mei Liang, Effect of source tampering in the security of quantum cryptography, *Phys. Rev. A* **92**, 022304 (2015).
- [17] Fadri Grünenfelder, Alberto Boaron, Davide Rusca, Anthony Martin, and Hugo Zbinden, Performance and security of 5 GHz repetition rate polarization-based quantum key distribution, *Appl. Phys. Lett.* **117**, 144003 (2020).
- [18] Shlok Nahar, Master's thesis, University of Waterloo, 2022.
- [19] Renato Renner, Security of quantum key distribution, *Int. J. Quantum Inf.* **6**, 1 (2008).
- [20] Charles H. Bennett, Gilles Brassard, and N. David Mermin, Quantum cryptography without Bell's theorem, *Phys. Rev. Lett.* **68**, 557 (1992).
- [21] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus, Entanglement as a precondition for secure quantum key distribution, *Phys. Rev. Lett.* **92**, 217903 (2004).
- [22] Nicky Kai Hong Li and Norbert Lütkenhaus, Improving key rates of the unbalanced phase-encoded BB84 protocol using the flag-state squashing model, *Phys. Rev. Res.* **2**, 043172 (2020).
- [23] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim, General paradigm for distilling classical key from quantum states, *IEEE Trans. Inf. Theory* **55**, 1898 (2009).
- [24] Renato Renner, Symmetry of large physical systems implies independence of subsystems, *Nat. Phys.* **3**, 645 (2007).
- [25] Matthias Christandl, Robert König, and Renato Renner, Postselection technique for quantum channels with applications to quantum cryptography, *Phys. Rev. Lett.* **102**, 020504 (2009).
- [26] Patrick J. Coles, Eric M. Metodiev, and Norbert Lütkenhaus, Numerical approach for unstructured quantum key distribution, *Nat. Commun.* **7**, 1 (2016).
- [27] Adam Winick, Norbert Lütkenhaus, and Patrick J. Coles, Reliable numerical key rates for quantum key distribution, *Quantum* **2**, 77 (2018).
- [28] Twesh Upadhyaya, Thomas van Himbeek, Jie Lin, and Norbert Lütkenhaus, Dimension reduction in quantum key distribution for continuous- and discrete-variable protocols, *PRX Quantum* **2**, 020325 (2021).
- [29] Nicky Kai Hong Li, Master's thesis, University of Waterloo, 2020.
- [30] Oleg Gittsovich, Normand J. Beaudry, Varun Narasimhachar, R. Romero Alvarez, Tobias Moroder, and Norbert Lütkenhaus, Squashing model for detectors and applications to quantum-key-distribution protocols, *Phys. Rev. A* **89**, 012325 (2014).
- [31] Daniel Gottesman, H.-K. Lo, Norbert Lutkenhaus, and John Preskill, in *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings.*, (IEEE, 2004), p. 136.
- [32] Zhu Cao, Zhen Zhang, Hoi-Kwong Lo, and Xiongfeng Ma, Discrete-phase-randomized coherent state source and its application in quantum key distribution, *New. J. Phys.* **17**, 053014 (2015).
- [33] Twesh Upadhyaya, Master's thesis, University of Waterloo, 2021.
- [34] Marcos Curty, Koji Azuma, and Hoi-Kwong Lo, Simple security proof of twin-field type quantum key distribution protocol, *npj Quantum Inf.* **5**, 1 (2019).
- [35] John Watrous, *The Theory of Quantum Information* (Cambridge university press, Cambridge, UK, 2018).
- [36] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussièeres, Ming-Jun Li, *et al.*, Secure quantum key distribution over 421 km of optical fiber, *Phys. Rev. Lett.* **121**, 190502 (2018).
- [37] Rajendra Bhatia, *Matrix Analysis* (Springer Science & Business Media, New York, New York, USA, 2013), Vol. 169.
- [38] Hoi-Kwong Lo, Marcos Curty, and Bing Qi, Measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [39] Guan-Jie Fan-Yuan, Feng-Yu Lu, Shuang Wang, Zhen-Qiang Yin, De-Yong He, Wei Chen, Zheng Zhou, Ze-Hao Wang, Jun Teng, Guang-Can Guo, *et al.*, Robust and adaptable quantum key distribution network without trusted nodes, *Optica* **9**, 812 (2022).
- [40] Marco Lucamarini, Zhiliang L. Yuan, James F. Dynes, and Andrew J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, *Nature* **557**, 400 (2018).
- [41] Shuang Wang, Zhen-Qiang Yin, De-Yong He, Wei Chen, Rui-Qiang Wang, Peng Ye, Yao Zhou, Guan-Jie Fan-Yuan, Fang-Xiang Wang, Wei Chen, *et al.*, Twin-field quantum key distribution over 830-km fibre, *Nat. Photonics* **16**, 154 (2022).
- [42] Elliott H. Lieb and Mary Beth Ruskai, Proof of the strong subadditivity of quantum-mechanical entropy, *Les Rencontres Physiciens-Mathématiciens de Strasbourg-RCP25* **19**, 36 (1973).
- [43] Tomohiro Ogawa and Hiroshi Nagaoka, in *Proceedings IEEE International Symposium on Information Theory.*, (IEEE, 2002), p. 73.
- [44] Gerald Teschl, Mathematical methods in quantum mechanics, *Grad. Stud. Math.* **99**, 106 (2009).
- [45] Daniel Hsu, Notes on matrix perturbation and Davis-Kahan $\sin \theta$ theorem, <https://www.cs.columbia.edu/djhsu/coms4772-f16/lectures/davis-kahan.pdf> (2016). Fall.
- [46] Varun Narasimhachar, Master's thesis, University of Waterloo, 2011.