

This is a repository copy of *Bounds on amplitude damping channel discrimination*.

White Rose Research Online URL for this paper:  
<https://eprints.whiterose.ac.uk/169747/>

Version: Accepted Version

---

**Article:**

Pereira, Jason L. and Pirandola, Stefano [orcid.org/0000-0001-6165-5615](https://orcid.org/0000-0001-6165-5615) (2021) Bounds on amplitude damping channel discrimination. *Physical Review A*. 022610. ISSN 1094-1622

<https://doi.org/10.1103/PhysRevA.103.022610>

---

**Reuse**

Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

**Takedown**

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing [eprints@whiterose.ac.uk](mailto:eprints@whiterose.ac.uk) including the URL of the record and the reason for the withdrawal request.

# Bounds on amplitude damping channel discrimination

Jason L. Pereira and Stefano Pirandola

*Department of Computer Science, University of York, York YO10 5GH, UK*

(Dated: December 4, 2020)

Amplitude damping (AD) channels are good models for many physical scenarios, and so the development of protocols to discriminate between them is an important task in quantum information science. It is therefore important to bound the performance of such protocols. Since adaptivity has been shown to improve the performance of discrimination protocols, bounds on the distinguishability of AD channels must take this into account. In this paper, we use both channel simulation and a bound based on the diamond norm to significantly tighten the upper bound on the trace norm between the possible outputs of binary channel discrimination protocols acting on AD channels (and hence the lower bound on the error probability of such protocols). The diamond norm between any two AD channels is found analytically, giving the optimal error probability for a one-shot discrimination protocol. We also present a tighter lower bound on the achievable trace norm between protocol outputs (and a corresponding upper bound on the achievable error probability). The upper and lower bounds are compared with existing bounds and then applied to quantum hacking and biological quantum sensing scenarios.

## I. INTRODUCTION

Quantum channel discrimination is the task of determining which quantum channel is present out of a set of possible channels. It is an important task in quantum information because it has many physical applications [1]. An example in quantum communications is quantum hacking [2–4], where Eve may wish to determine aspects of the settings of Alice’s and Bob’s devices, by probing them via side-channels. If the settings affect the quantum channel that the probes would pass through, Eve could carry out a discrimination protocol between the possible channels, and therefore the possible settings.

Within quantum channel discrimination, one well-studied task is binary discrimination. This is discrimination between only two possible channels. For equal prior probabilities, the error probability in distinguishing between the two possible output states of a discrimination protocol is known exactly, in terms of the trace norm (the Helstrom bound) [5]. One application of binary discrimination is in quantum illumination [6–19], where a device must discriminate between the presence and the absence of an object. Another application is the protocol of quantum reading [20] (see the recent review [1] and references therein).

Adaptive protocols, where subsequent probes can be dependent on measurements carried out on previous probes, have proven to be more powerful than non-adaptive protocols for certain pairs of channels [21]. Note that this is not the case for all channels: adaptivity has been shown to be unnecessary for discriminating between unitary channels [22] and to not help the asymptotic error rate for discriminating between classical channels [23]. Nonetheless, for pairs of channels that have not been proven to not require adaptivity for optimal discrimination, adaptivity must be taken into account. This has necessitated the study of the most general adaptive protocols, in order to establish ultimate bounds on the minimum achievable error probability for quantum channel discrimination [1]. Quantum channel simulation is a powerful tool for establishing these ultimate bounds [24–28].

Pure loss channels constitute an important class of quantum channels. They can be used as models in many situations

in which the environmental noise is low. Examples include quantum communications [24] and quantum metrology [29] (where the parameter being measured could be the loss of the channel). Amplitude damping (AD) channels are qubit channels that act similarly to lossy channels: they can be regarded as lossy channels that only act on qubit states. In physics, they are good models for energy dissipation in qubit systems [30], and in quantum information, they can model low noise scenarios where the number of photons passing through a quantum channel is also low. They have also been used as a model for the transfer of a qubit through a spin chain [31].

AD channel discrimination was briefly discussed in Ref. [25]. The authors presented a lower bound on the discrimination error of adaptive protocols based on channel simulation using port-based teleportation (PBT) and an upper bound based on (non-adaptive) probing with Bell states. Ref. [32] investigated the multiple channel discrimination case (i.e. discrimination between more than two possible channels) of channel position finding over a sequence of AD channels. Ref. [33] investigated adaptive discrimination of generalised amplitude damping channels (which can be reduced to AD channel discrimination by setting the noise parameter to 0) and Ref. [34] presented results relating to AD channel discrimination.

In this work, we find various upper bounds on the trace norm between the possible output states of any adaptive discrimination protocol that is discriminating between AD channels. We therefore lower bound the optimal error probabilities for binary discrimination tasks between AD channels. We present two new upper bounds based on PBT channel simulation, with different resource states from those used in Ref. [25], and an upper bound based on the diamond norm. The latter bound is also applicable to a wider variety of discrimination tasks. We give an analytical expression for the exact diamond norm between any pair of AD channels. We present a tighter lower bound on the optimal trace norm for discrimination protocols between AD channels, which is well approximated by an approximate bound based on the quantum Cramér-Rao bound (QCRB), given in Ref. [35], for a large number of channel uses.

We numerically investigate the presented bounds, and com-

pare them with the existing bounds found in Ref. [25]. We then apply the bounds to a quantum hacking scenario, in which Eve is attempting to learn Alice's bases for BB84, using a side-channel. We also apply the bounds to a biological quantum metrology scenario, in which a sample must be probed with low energy quantum states, in order to detect the presence of bacteria or to discriminate between two types of bacteria.

In Section II, we describe the task of binary AD channel discrimination via an adaptive protocol and present the various bounds. We also calculate the diamond norm between AD channels. In Section III, we compare the bounds with existing bounds and apply them to two different scenarios. Finally, in Section IV, we present our conclusions.

## II. ANALYTICAL RESULTS

Suppose we are given an AD channel,  $\mathcal{C}$ , which we know to have a transmissivity,  $\eta$ , equal to either  $\eta_X$  or  $\eta_Y$ , and wish to determine which of these two values  $\eta$  takes. AD channels are qubit channels and are defined by having the Kraus operators

$$K_0 = |0\rangle\langle 0| + \sqrt{\eta}|1\rangle\langle 1|, \quad (1)$$

$$K_1 = \sqrt{1-\eta}|0\rangle\langle 1|. \quad (2)$$

Equivalently, they can be described by the Choi matrix

$$C_{\text{AD}} = \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{\sqrt{\eta}}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1-\eta}{2} & 0 \\ \frac{\sqrt{\eta}}{2} & 0 & 0 & \frac{\eta}{2} \end{pmatrix}. \quad (3)$$

The Choi matrix of a qubit channel is the state obtained by sending one half of a Bell pair through the channel. In this case, the Bell pair being used is  $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ ; in the context of Choi resources for PBT (as discussed in detail in Subsection IIF), the Bell pair used to generate Choi matrices is  $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ .

Note that an AD channel is the qubit version of a pure loss channel, in that the pointwise application of a hard energy constraint of one photon and a pure loss channel with transmissivity  $\eta$  reduces to an AD channel with transmissivity  $\eta$  (or damping probability  $1 - \eta$ ). Suppose we are allowed to carry out any protocol involving our channel, but with a maximum of  $N$  channel uses. Let  $\mathcal{C}_X$  be the AD channel with a transmissivity of  $\eta_X$  and let  $\mathcal{C}_Y$  be the AD channel with a transmissivity of  $\eta_Y$ . Our task is to carry out the optimal protocol for discriminating between  $\mathcal{C}_X$  and  $\mathcal{C}_Y$ , subject to the constraint on the total number of channel uses.

A general protocol consists of quantum operations on some initial state, followed by a channel use, followed by further operations (which can include measurements) and further channel uses, until a total of  $N$  channel uses have occurred [25]. Note that the initial state can be arbitrarily large and may include idler modes. At this point, a final set of quantum operations is carried out, and then a measurement is made on the final state, which we will label as  $\rho_i^{N,\text{out}}$  in the case in

which the channel is  $\mathcal{C}_i$ . Note that this protocol is allowed to be adaptive, meaning that each step in the protocol can depend on previous steps. We define the optimal protocol as the protocol for which we maximise the trace norm between  $\rho_X^{N,\text{out}}$  and  $\rho_Y^{N,\text{out}}$  and then carry out the most discriminating measurement possible. This optimal value of the trace norm is denoted by  $D_{\mathcal{C}_X\mathcal{C}_Y}^{\text{opt},N}$ . If we have  $\mathcal{C}_X$  and  $\mathcal{C}_Y$  with equal probabilities, this is the protocol that minimises the probability of error in identifying which channel we have. It is also worth noting that, for the optimal protocol, we can assume without loss of generality that all of the operations between channel uses are unitaries, as any other operations (such as quantum channels, of which measurements are a special case) can be modelled as unitaries, by allowing the user of the protocol to hold the distillation of all operations performed. This cannot decrease the trace distance between output states.

### A. Bounding the maximum trace norm using channel simulation

We now apply the technique of channel simulation [24, 25, 28]. Suppose we have a qubit quantum processor  $\mathcal{Q}(\pi)$ , which takes the resource state  $\pi$  as a program and enacts the channel  $\mathcal{C}_{\mathcal{Q}(\pi)}$  on an input qubit, via some set of trace-preserving quantum operations. Suppose also that there exist program states  $\pi_X$  and  $\pi_Y$ , such that the enacted channels,  $\mathcal{C}_{\mathcal{Q}(\pi_X)}$  and  $\mathcal{C}_{\mathcal{Q}(\pi_Y)}$ , are sufficiently close to the two AD channels that we want to discriminate between. More precisely, suppose we can write

$$\|\mathcal{C}_{\mathcal{Q}(\pi_X)} - \mathcal{C}_X\|_{\diamond} \leq \epsilon_X, \quad (4)$$

$$\|\mathcal{C}_{\mathcal{Q}(\pi_Y)} - \mathcal{C}_Y\|_{\diamond} \leq \epsilon_Y, \quad (5)$$

where we have used the diamond norm between the channels. This is the maximum of the trace norm between the outputs of the channels, maximised over all input states (including those with idlers). Then, we replace the  $N$  channel uses in our discrimination protocol with the channel enacted by the processor (with program state  $\pi_{X(Y)}$  in the case in which the channel is  $\mathcal{C}_{X(Y)}$ ), and call the output state of the resulting protocol  $\rho_{\mathcal{Q}(\pi_{X(Y)})}^{N,\text{out}}$ . By using the contractivity of the trace norm under quantum channels and the triangle inequality (see Subsection IIC for a more detailed derivation along similar lines), we can then write

$$\left\| \rho_{\mathcal{Q}(\pi_X)}^{N,\text{out}} - \rho_X^{N,\text{out}} \right\|_1 \leq N\epsilon_X, \quad (6)$$

$$\left\| \rho_{\mathcal{Q}(\pi_Y)}^{N,\text{out}} - \rho_Y^{N,\text{out}} \right\|_1 \leq N\epsilon_Y. \quad (7)$$

Using the fact that all of the operations are trace-preserving, and the only difference between the two cases is the initial program state, we can write

$$\left\| \rho_{\mathcal{Q}(\pi_X)}^{N,\text{out}} - \rho_{\mathcal{Q}(\pi_Y)}^{N,\text{out}} \right\|_1 \leq \left\| \pi_X^{\otimes N} - \pi_Y^{\otimes N} \right\|_1 \quad (8)$$

$$\leq 2\sqrt{1 - F(\pi_X^{\otimes N}, \pi_Y^{\otimes N})^2}, \quad (9)$$

where  $F(\rho_1, \rho_2)$  is the quantum fidelity, defined by

$$F(\rho_1, \rho_2) = \text{Tr} \sqrt{\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}}. \quad (10)$$

When bounding the trace norm between  $N$  copies of each program state, one might also consider using the quantum Chernoff bound (QCB) [36]. The QCB in the non-logarithmic form is defined by

$$Q(\rho_1, \rho_2) = \min_{0 \leq s \leq 1} \text{Tr} [\rho_1^s \rho_2^{1-s}]. \quad (11)$$

We can then bound the trace norm between two states,  $D$ , with

$$2(1 - Q) \leq D \leq 2\sqrt{1 - Q^2}. \quad (12)$$

Note that  $Q(\rho_1, \rho_2) < F(\rho_1, \rho_2)$  [37]. Since we are interested in upper bounding the trace norm between two program states, the Fuchs-van der Graaf relation (in Eq. (9)) gives a tighter bound (although the QCB gives a tighter lower bound).

Using the multiplicativity of the fidelity with respect to tensor products, we get

$$\left\| \rho_{\mathcal{Q}(\pi_X)}^{N, \text{out}} - \rho_{\mathcal{Q}(\pi_Y)}^{N, \text{out}} \right\|_1 \leq 2\sqrt{1 - F(\pi_X, \pi_Y)^{2N}}. \quad (13)$$

Finally, using the triangle inequality, we write

$$D_{\mathcal{C}_X \mathcal{C}_Y}^{\text{opt}, N} \leq N\epsilon_{XY} + 2\sqrt{1 - F(\pi_X, \pi_Y)^{2N}}, \quad (14)$$

$$\epsilon_{XY} = \epsilon_X + \epsilon_Y, \quad (15)$$

where  $D_{\mathcal{C}_X \mathcal{C}_Y}^{\text{opt}, N}$  is maximised over all possible protocols.

The trace norm between two states is related to the maximum probability of successfully discriminating between them,  $p^{\text{succ}}$  via

$$p^{\text{succ}} = \frac{1}{2} + \frac{D}{4}, \quad (16)$$

and so we have an upper bound on the probability of discriminating between two amplitude damping channels  $\mathcal{C}_X$  and  $\mathcal{C}_Y$ , which holds over all possible adaptive protocols. Alternatively, by defining

$$p^{\text{err}} = 1 - p^{\text{succ}} \quad (17)$$

$$= \frac{1}{2} - \frac{D}{4}, \quad (18)$$

we have a lower bound on the error probability.

Note that the tightness of this bound depends both on the chosen program states,  $\pi_X$  and  $\pi_Y$ , and on the quantum processor,  $\mathcal{Q}$ , used. In order to attain a tight bound, we need to both minimise the simulation errors,  $\epsilon_X$  and  $\epsilon_Y$ , and minimise the trace norm between the program states simultaneously. For instance, we could conceive of a trivial quantum processor that measures the program state in the computational basis and then, depending on the outcome of the measurement, enacts either  $\mathcal{C}_X$  or  $\mathcal{C}_Y$ . Choosing the program states  $|0\rangle$  and  $|1\rangle$ , we get  $\epsilon_{X(Y)} = 0$ , but the trace norm between the program states is maximised, and hence our bound is too large. More useful bounds can be found with processors that use PBT, as discussed in Subsection II B, and with a different trivial processor, as discussed in Subsection II C.

## B. Quantum processors for AD channel simulation

As previously mentioned, the tightness of the bound depends on the quantum processor and program states used to simulate the channels. We wish to minimise the simulation error whilst keeping our program states as similar to each other as possible, in order to achieve the tightest possible bound.

One idea that may be intuitively appealing is to use (standard) quantum teleportation [38] to simulate the AD channels. For certain qubit channels (namely, Pauli channels), quantum teleportation using the Choi matrix of the channel as a resource (program state) can perfectly simulate the channel (with a simulation error of 0).

The issue with this is that standard quantum teleportation cannot simulate non-Pauli channels [39], and so we would have a very high simulation error. This would result in a bound that would be too loose to be useful.

One alternative is to use port-based teleportation [40, 41]. PBT uses a combined measurement (the square-root measurement) on an input state and  $m$  ports, held by the sender, to teleport the input state to one of  $m$  ports, held by the receiver. The receiver then traces over the remaining ports. The process is discussed in more detail in Refs. [40–42]. The program state is the shared resource state of  $2m$  qubits,  $m$  of which constitute the sender's ports and  $m$  of which constitute the receiver's ports.

A possible program state, in this case, is  $m$  copies of the Choi matrix of the AD channel. It is known that in the asymptotic limit of  $m \rightarrow \infty$ , such a simulation becomes perfect. The issue with this is that the trace norm between the program states of the two possible channels increases as the number of copies increases, and so we cannot take the asymptotic limit of  $m$ . Instead, we can accept some small but non-zero simulation error, and try to find the optimal value of  $m$  to minimise the total value of the bound.

This is the approach taken by Ref. [25], for calculating a lower bound for the error probability of discriminating between two AD channels (i.e. the same type of bound that we want to calculate here). We will call the family of bounds that come from PBT simulations using the Choi matrix of the simulated channels as a resource the standard Choi bounds (and will implicitly assume that the optimal value of  $m$  has been chosen).

In fact, for finite  $m$ , there are program states that simulate AD channels better than  $m$  copies of the Choi matrix of the simulated channel. This was discussed in Ref. [42], in which two classes of resource states capable of providing better simulations of AD channels were presented.

The first class uses  $m$  copies of the Choi matrix of a different AD channel from the one being simulated as a resource. Specifically, to simulate an AD channel with transmissivity  $\eta$ , we use  $m$  copies of the Choi matrix of the AD channel with transmissivity  $\eta'$ , where

$$\eta' = \frac{\eta}{1 - \xi_m}. \quad (19)$$

$\xi_m$  is the PBT coefficient for  $m$  ports, as defined in Eq. (11) of Ref. [25], and represents the depolarisation probability when

carrying out PBT with a maximally entangled resource state. As such, it is a number between 0 and 1, and consequently  $\eta' > \eta$ . Our notation here differs from Ref. [42], since we are characterising the AD channels with  $\eta$  rather than the damping probability (which is  $1 - \eta$ ). Note that we also require  $\eta \leq 1 - \xi_m$ . We will call the bounds deriving from PBT using this resource state the improved Choi bounds.

The second class uses pure resource states, parametrised by a parameter  $a$ , that take the form

$$R^{alt}(a) = (\sqrt{a}|01\rangle - \sqrt{1-a}|10\rangle)^{\otimes m}. \quad (20)$$

An advantage that comes from the fact that this resource state is pure is that the trace distance between different program states is analytically calculable (since the upper bound coming from the fidelity is tight). The value of the parameter  $a$  is determined by both the damping probability of the AD channel that is being simulated and by the number of ports,  $m$ , and is chosen so as to minimise the simulation error. We will call the bounds deriving from PBT using this resource state the alternative resource bounds.

The upper bounds based on program states of these types are calculated in Subsection II F. In all three cases, we must tune  $m$  so as to obtain the tightest bound possible.

### C. The trivial bound

We can also formulate a bound based on a trivial processor that simply always enacts the channel  $\mathcal{C}_X$ . In this case, we have

$$\epsilon_X = 0, \quad (21)$$

$$\epsilon_Y = \|\mathcal{C}_X - \mathcal{C}_Y\|_\diamond, \quad (22)$$

$$\|\pi_X^{\otimes M} - \pi_Y^{\otimes M}\|_1 = 0. \quad (23)$$

In other words, the bound in Eq. (15) simply becomes

$$D_{\mathcal{C}_X \mathcal{C}_Y}^{\text{opt}, N} \leq ND_{\mathcal{C}_X \mathcal{C}_Y}^\diamond, \quad (24)$$

$$D_{\mathcal{C}_X \mathcal{C}_Y}^\diamond = \|\mathcal{C}_X - \mathcal{C}_Y\|_\diamond. \quad (25)$$

This is  $N$  times the diamond distance between the two channels that we are trying to distinguish between. Note that this bounds is not specific to AD channels, and could be applied to any binary discrimination task.

In fact, we can write an alternative and simpler proof that this bound holds. Let

$$S(N, m) = \{\mathcal{C}_X, \mathcal{C}_X, \dots, \mathcal{C}_X, \mathcal{C}_Y, \mathcal{C}_Y, \dots, \mathcal{C}_Y\} \quad (26)$$

be a sequence of  $N$  channels that are either  $\mathcal{C}_X$  or  $\mathcal{C}_Y$ . Specifically, the first  $m$  channels are  $\mathcal{C}_X$  and the next  $N - m$  channels are  $\mathcal{C}_Y$ . Then let  $\mathcal{P}(S(N, m))$  be the output of a fully general and potentially adaptive protocol  $\mathcal{P}$ , which has a total of  $N$  channel uses, where the  $i$ -th channel use involves sending the signal through the channel that is the  $i$ -th element of  $S$ . E.g. if  $S(3, 2) = \mathcal{C}_X, \mathcal{C}_X, \mathcal{C}_Y$ ,  $\mathcal{P}(S)$  is the output of a discrimination protocol when the channel that we are trying to identify

as either  $\mathcal{C}_X$  or  $\mathcal{C}_Y$  (and which the protocol assumes is always the same) is  $\mathcal{C}_X$  for the first two channel uses and is  $\mathcal{C}_Y$  for the final channel use. We then have

$$\mathcal{P}(S(N, N)) = \mathcal{P}(\mathcal{C}_X, \mathcal{C}_X, \dots, \mathcal{C}_X) = \rho_X^{N, \text{out}}, \quad (27)$$

$$\mathcal{P}(S(N, 0)) = \mathcal{P}(\mathcal{C}_Y, \mathcal{C}_Y, \dots, \mathcal{C}_Y) = \rho_Y^{N, \text{out}}. \quad (28)$$

We therefore want to upper bound the trace distance between  $\mathcal{P}(S(N, N))$  and  $\mathcal{P}(S(N, 0))$ . We start by writing

$$\|\mathcal{P}(S(N, N)) - \mathcal{P}(S(N, N-1))\|_1 \leq D_{\mathcal{C}_X \mathcal{C}_Y}^\diamond. \quad (29)$$

This is due to the fact that the states are identical prior to the final channel use, the states immediately after the final channel use cannot be further apart than the diamond distance between the two channels and any subsequent post-processing is the same in both cases, and so cannot increase the trace distance between the states.

By a similar argument we have

$$\|\mathcal{P}(S(N, N-1)) - \mathcal{P}(S(N, N-2))\|_1 \leq D_{\mathcal{C}_X \mathcal{C}_Y}^\diamond, \quad (30)$$

and generalising, we can write

$$\|\mathcal{P}(S(N, i)) - \mathcal{P}(S(N, i-1))\|_1 \leq D_{\mathcal{C}_X \mathcal{C}_Y}^\diamond. \quad (31)$$

Then, using the triangle inequality, we can write

$$\|\mathcal{P}(S(N, i)) - \mathcal{P}(S(N, i-j))\|_1 \leq (i-j)D_{\mathcal{C}_X \mathcal{C}_Y}^\diamond, \quad (32)$$

and therefore

$$\|\mathcal{P}(S(N, N)) - \mathcal{P}(S(N, 0))\|_1 \leq ND_{\mathcal{C}_X \mathcal{C}_Y}^\diamond, \quad (33)$$

as required.

The diamond norm between any two AD channels is presented in Subsection II D.

### D. Calculating the diamond norm between two AD channels

We start by making an ansatz that the exact diamond norm between two AD channels can be achieved using a state of the form

$$|\phi(t)\rangle = \sqrt{t}|00\rangle + \sqrt{1-t}|11\rangle, \quad (34)$$

where  $0 \leq t \leq 1$ . The trace norm between two AD channels for such a state,  $D_{\mathcal{C}_X \mathcal{C}_Y}^{|\phi(t)\rangle, 1}$ , is then given by

$$D_{\mathcal{C}_X \mathcal{C}_Y}^{|\phi(t)\rangle, 1} = |\eta_X - \eta_Y|(1-t) \left( 1 + \sqrt{1 + \frac{4t}{(1-t)x^2}} \right), \quad (35)$$

$$x = \sqrt{\eta_X} + \sqrt{\eta_Y}. \quad (36)$$

Defining  $t_{\max}$  as the value of  $t$  that maximises  $D_{\mathcal{C}_X \mathcal{C}_Y}^{|\phi(t)\rangle, 1}$ , we find

$$t_{\max} = \max\left\{0, 1 - \frac{1}{2-x}\right\}. \quad (37)$$

From this, we can see that the problem is split into two regimes: one in which  $t_{\max} = 0$  and one in which  $t_{\max} > 0$ . Note that for the extremal case of  $t = 0$ , the idler mode is not necessary, since the state given by Eq. (34) is separable for this parameter value. Consequently, probing with  $|1\rangle$  is equivalent to probing with  $|11\rangle$ . The first regime occurs when

$$\sqrt{\eta_x} + \sqrt{\eta_y} > 1. \quad (38)$$

We can then calculate the trace norms for each regime:

$$D_{\mathcal{C}_X \mathcal{C}_Y}^{\diamond, t=0} = 2|\eta_X - \eta_Y|, \quad (39)$$

$$D_{\mathcal{C}_X \mathcal{C}_Y}^{\diamond, t>0} = \frac{2|\sqrt{\eta_X} - \sqrt{\eta_Y}|}{2 - (\sqrt{\eta_X} + \sqrt{\eta_Y})}. \quad (40)$$

The next step is to prove that the expressions in Eqs. (39) and (40) are the diamond norms in each regime. We do this using semidefinite programming. Ref. [43] showed that finding the diamond norm can be reduced to a semidefinite programming problem. In a semidefinite programming problem, some matrices must be chosen, subject to constraints, to maximise or minimise a quantity that is dependent on these matrices. More specifically, every problem consists of a primal and a dual problem. Each valid solution to the primal problem provides a lower bound to the quantity, and so one maximises over the primal problem. Each valid solution to the dual problem provides an upper bound to the quantity, and so one minimises over it. Therefore, in order to show that Eqs. (39) and (40) give the diamond norm, we must find matrices satisfying the constraints of the dual problem for the diamond norm that give the expressions in Eqs. (39) and (40) as the diamond norm. The dual problem is to find positive matrices  $Y_0$  and  $Y_1$  that satisfy the constraint

$$M = \begin{pmatrix} Y_0 & -J(\mathcal{C}_X, \mathcal{C}_Y) \\ -J(\mathcal{C}_X, \mathcal{C}_Y) & Y_1 \end{pmatrix} > 0, \quad (41)$$

where  $J$  is the Choi matrix of channel  $\mathcal{C}_X$  minus the Choi matrix of channel  $\mathcal{C}_Y$ , multiplied by the dimension of the input system (which, in our case, is 2). The upper bound on the diamond norm, which we must then minimise, is

$$D_{\mathcal{C}_X \mathcal{C}_Y}^{\diamond} \leq \frac{\|\text{Tr}_S(Y_0)\|_{\infty} + \|\text{Tr}_S(Y_1)\|_{\infty}}{2}, \quad (42)$$

where the partial trace is taken over the signal (rather than the idler) mode, and the norm is the operator norm (i.e. the largest eigenvalue). In our case, we have

$$J(\mathcal{C}_X, \mathcal{C}_Y) = \begin{pmatrix} 0 & 0 & 0 & \sqrt{\eta_X} - \sqrt{\eta_Y} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \eta_Y - \eta_X & 0 \\ \sqrt{\eta_X} - \sqrt{\eta_Y} & 0 & 0 & \eta_X - \eta_Y \end{pmatrix}. \quad (43)$$

Let us first consider the  $t = 0$  case. Consider the matrices

$$Y_0^{t=0} = \begin{pmatrix} D_{\mathcal{C}_X \mathcal{C}_Y}^{\diamond, t=0} & 0 & 0 & |\sqrt{\eta_X} - \sqrt{\eta_Y}| \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2}D_{\mathcal{C}_X \mathcal{C}_Y}^{\diamond, t=0} & 0 \\ |\sqrt{\eta_X} - \sqrt{\eta_Y}| & 0 & 0 & \frac{1}{2}D_{\mathcal{C}_X \mathcal{C}_Y}^{\diamond, t=0} \end{pmatrix}, \quad (44)$$

$$Y_1^{t=0} = Y_0^{t=0}. \quad (45)$$

We can immediately see that

$$\text{Tr}_S(Y_0^{t=0}) = \text{Tr}_S(Y_1^{t=0}) = D_{\mathcal{C}_X \mathcal{C}_Y}^{\diamond, t=0} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (46)$$

and so the upper bound on the diamond norm coming from this solution is equal to the expression in Eq. (39). The distinct, non-zero eigenvalues of  $M^{t=0}$  are

$$e_{M^{t=0}}^1 = 2|\eta_X - \eta_Y|, \quad (47)$$

$$e_{M^{t=0}}^2 = 2(|\eta_X - \eta_Y| - |\sqrt{\eta_X} - \sqrt{\eta_Y}|), \quad (48)$$

$$e_{M^{t=0}}^3 = 2(|\eta_X - \eta_Y| + |\sqrt{\eta_X} - \sqrt{\eta_Y}|), \quad (49)$$

the smallest of which is  $e_{M^{t=0}}^2$ . Since  $e_{M^{t=0}}^2 > 0$  for the regime in which  $t = 0$  (i.e. for  $x > 1$ ),  $M^{t=0} > 0$  in this regime, as required. The non-zero eigenvalues of  $Y_0^{t=0}$  (and  $Y_1^{t=0}$ ) are

$$e_{Y^{t=0}}^1 = |\eta_X - \eta_Y|, \quad (50)$$

$$e_{Y^{t=0}}^2 = \frac{|\eta_X - \eta_Y|}{2} \left( 3 - \sqrt{1 + \frac{4}{x^2}} \right), \quad (51)$$

$$e_{Y^{t=0}}^3 = \frac{|\eta_X - \eta_Y|}{2} \left( 3 + \sqrt{1 + \frac{4}{x^2}} \right). \quad (52)$$

$e_{Y^{t=0}}^2$  is the smallest of these, and  $e_{Y^{t=0}}^2 > 0$  in the regime in which  $t = 0$ , so both  $Y_0^{t=0}$  and  $Y_1^{t=0}$  are positive. Therefore, Eq. (39) gives the exact diamond norm for the  $t = 0$  regime.

Next, we consider the  $t > 0$  case. Consider the matrices

$$Y_0^{t>0} = \begin{pmatrix} D_{\mathcal{C}_X \mathcal{C}_Y}^{\diamond, t>0} & 0 & 0 & \frac{|\eta_X - \eta_Y|}{2-x} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2}D_{\mathcal{C}_X \mathcal{C}_Y}^{\diamond, t=0} & 0 \\ \frac{|\eta_X - \eta_Y|}{2-x} & 0 & 0 & D_{\mathcal{C}_X \mathcal{C}_Y}^{\diamond, t>0} - \frac{1}{2}D_{\mathcal{C}_X \mathcal{C}_Y}^{\diamond, t=0} \end{pmatrix}, \quad (53)$$

$$Y_1^{t>0} = Y_0^{t>0}. \quad (54)$$

Tracing over the signal mode, we get

$$\text{Tr}_S(Y_0^{t>0}) = \text{Tr}_S(Y_1^{t>0}) = D_{\mathcal{C}_X \mathcal{C}_Y}^{\diamond, t>0} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (55)$$

and so the upper bound on the diamond norm coming from this solution is equal to the expression in Eq. (40). The non-zero eigenvalues of  $M^{t>0}$  are

$$e_{M^{t=0}}^1 = 2|\eta_X - \eta_Y|, \quad (56)$$

$$e_{M^{t=0}}^2 = \frac{4|\sqrt{\eta_X} - \sqrt{\eta_Y}|}{2-x}, \quad (57)$$

$$e_{M^{t=0}}^3 = \frac{4|\sqrt{\eta_X} - \sqrt{\eta_Y}|}{2-x} - 2|\eta_X - \eta_Y|, \quad (58)$$

which are all positive. The non-zero eigenvalues of  $Y_0^{t>0}$  (and

$Y_1^{t>0}$ ) are

$$e_{Y^{t>0}}^1 = |\eta_X - \eta_Y|, \quad (59)$$

$$e_{Y^{t>0}}^2 = \frac{|\sqrt{\eta_X} - \sqrt{\eta_Y}|}{2(2-x)} \left( 3 + (1-x)^2 - x\sqrt{4+(2-x)^2} \right), \quad (60)$$

$$e_{Y^{t>0}}^3 = \frac{|\sqrt{\eta_X} - \sqrt{\eta_Y}|}{2(2-x)} \left( 3 + (1-x)^2 + x\sqrt{4+(2-x)^2} \right). \quad (61)$$

These are again all positive, proving that Eq. (40) gives the exact diamond norm for the  $t > 0$  regime.

A logical next step would be to calculate the diamond norm between multiple uses of two AD channels, i.e. between the two channels  $\mathcal{C}_X^{\otimes N}$  and  $\mathcal{C}_Y^{\otimes N}$ . However, this is a more difficult task. Numerically, we find that input states of the form  $|1\rangle^{\otimes N}$  achieve the diamond norm in some cases, as for the single use case, but that the regimes are more complicated to characterise. Further, for large numbers of channel uses, numerically finding the diamond norm via semidefinite programming is computationally expensive.

### E. Lower bounds on the optimal trace norm

It is helpful to also find lower bounds on the maximum trace distance between protocol outputs,  $D_{\mathcal{C}_X \mathcal{C}_Y}^{\text{opt}, N}$  since this allows us to assess how tight our upper bounds are. One option is to find the diamond norm between  $\mathcal{C}_X^{\otimes N}$  ( $N$  copies of  $\mathcal{C}_X$ ) and  $\mathcal{C}_Y^{\otimes N}$ . The only reason that such a lower bound would not be tight is if adaptivity between rounds adds to the discriminative power of a protocol (it is not yet known whether this is the case). The problem with using such a bound is that it is difficult to find the diamond norm for  $N > 1$  (as discussed in Subsection IID).

An alternative is to consider specific protocols that could be implemented and to find the trace distances between outputs in these cases. Since we are looking for the maximum trace distance over all possible protocols, any specific protocol provides a lower bound on this maximum.

Ref. [25] provided a lower bound on the trace norm between protocol outputs, based on consideration of a non-adaptive protocol, in which  $N$  copies of a Bell state are sent through the channel. The output of this protocol is  $N$  copies of the Choi matrix of the channel. It was shown that

$$D_{\mathcal{C}_X \mathcal{C}_Y}^{\text{opt}, N} \geq 2 \left( 1 - f^{\text{Choi}}(\eta_X, \eta_Y)^N \right), \quad (62)$$

$$f^{\text{Choi}}(p, q) = \frac{1 + \sqrt{(1-p)(1-q)} + \sqrt{pq}}{2}. \quad (63)$$

$f^{\text{Choi}}$  is the fidelity between the Choi matrices of channels  $\mathcal{C}_X$  and  $\mathcal{C}_Y$ . We refer to this as the Bell state lower bound.

In fact, we find that we can obtain a slightly tighter bound using an alternative, non-adaptive protocol, in which  $N$  copies of the state  $|1\rangle$  are sent through the channel. Note that this

is also the input state that achieves the maximum quantum Fisher information (QFI) per channel use [44], and so is the optimal input state for parameter estimation, at least in the asymptotic limit of a large number of channel uses. In this case, we obtain the tighter bound

$$D_{\mathcal{C}_X \mathcal{C}_Y}^{\text{opt}, N} \geq 2 \left( 1 - f^{(1)}(\eta_X, \eta_Y)^N \right), \quad (64)$$

$$f^{(1)}(p, q) = \sqrt{(1-p)(1-q)} + \sqrt{pq}. \quad (65)$$

This bound is again based on the fidelity between the possible outputs of the protocol.

For sufficiently small  $N$ , we can do better still by calculating the exact trace norm for this protocol (rather than lower bounding it). Since the output state of the protocol takes the form

$$\rho_{X(Y)}^{N, \text{out}} = ((1 - \eta_{X(Y)}) |0\rangle\langle 0| + \eta_{X(Y)} |1\rangle\langle 1|)^{\otimes N}, \quad (66)$$

for channel  $\mathcal{C}_{X(Y)}$ , the trace norm between the two possible outputs,  $D_{\mathcal{C}_X \mathcal{C}_Y}^{(1), N}$ , is

$$D_{\mathcal{C}_X \mathcal{C}_Y}^{(1), N} = \sum_{i=0}^N \binom{N}{i} \left| \eta_X^{N-i} (1 - \eta_X)^i - \eta_Y^{N-i} (1 - \eta_Y)^i \right|. \quad (67)$$

We will refer to this bound as the improved lower bound. The problem with using this bound for large  $N$  is that the binomial coefficients become large, and therefore computationally difficult to calculate.

When applying the trace norm bounds to channel discrimination, the improved lower bound can be approximated using the quantum Cramér-Rao bound, as per Ref. [35]. The QCRB lower bounds the error-variance for estimating a channel parameter, based on the QFI with respect to that parameter. In our case, we have

$$\sigma_\eta^2 \leq \frac{1}{NH_\eta}, \quad (68)$$

where  $\sigma_\eta^2$  is the variance of an estimation of  $\eta$  around its true value and  $H_\eta$  is the QFI with respect to  $\eta$ . As shown in Ref. [44], the optimal QFI is achieved using number states with the maximum number of photons per channel use. In our case, this is the state  $|1\rangle$  and the maximum QFI per channel use is

$$H_\eta^{\text{max}} = \frac{1}{\eta(1-\eta)}. \quad (69)$$

The QCRB therefore takes the form

$$\sigma_\eta^2 \leq \frac{\eta(1-\eta)}{N}. \quad (70)$$

We can return to a binary hypothesis testing scenario by picking a threshold value,  $\tau$ , of  $\eta$ , such that if our estimation of  $\eta$  is greater than  $\tau$ , we decide that we have channel  $\mathcal{C}_X$  (for  $\eta_X > \eta_Y$ ), and if not, we decide that we have channel  $\mathcal{C}_Y$ . We assume that our estimation of  $\eta$ ,  $\eta'$ , follows a Gaussian

probability distribution, centred on the true value of  $\eta$ , with a variance equal to the lower bound from Eq. (70). For  $\mathcal{C}_{X(Y)}$ , this distribution is given by

$$p_{\eta_{X(Y)}}(\eta') = \frac{1}{\sigma_\eta \sqrt{2\pi}} e^{-\frac{(\eta' - \eta_{X(Y)})^2}{2\sigma_\eta^2}}. \quad (71)$$

Ref. [35] then calculated the probabilities of deciding we have channel  $\mathcal{C}_Y$  when we have channel  $\mathcal{C}_X$  ( $p_X^{\text{err}}$ ) and of deciding we have channel  $\mathcal{C}_X$  when we have channel  $\mathcal{C}_Y$  ( $p_Y^{\text{err}}$ ). These error probabilities are

$$p_X^{\text{err}} = \mathcal{N}_X^{-1} \int_0^\tau p_{\eta_X}(\eta') d\eta', \quad (72)$$

$$p_Y^{\text{err}} = \mathcal{N}_Y^{-1} \int_\tau^1 p_{\eta_Y}(\eta') d\eta', \quad (73)$$

$$\mathcal{N}_{X(Y)} = \int_0^1 p_{\eta_{X(Y)}}(\eta') d\eta', \quad (74)$$

where the normalisation factors,  $\mathcal{N}_{X(Y)}$ , are due to restricting the probability distributions to the range  $[0, 1]$ , and again assuming  $\eta_X > \eta_Y$ . In the case in which both channels have prior probabilities, we can then choose the value of  $\tau$  that minimises the mean of these two errors, in order to find the total error probability (in the asymmetric case, we can minimise a weighted mean of the errors). This then gives us an estimate of the error probability obtained using the improved lower bound on the trace norm.

It should be noted that this estimate is only tight for a large number of channel uses. For a small number of channel uses, the QCRB is often not tight [45]. Since Eq. (70) lower bounds the variance of the parameter estimates (rather than upper bounding them), we do not attain an upper bound on the error probability, but rather an estimate of the error probability attained using the upper bound in Eq. (67) (since we are using the same input states in both cases, and the trace norm between the output states gives the lowest possible error in discriminating between them). In fact, for low  $N$ , the estimate of the bound based on the QCRB, which we will call the QCRB bound, underestimates the minimum error probability over a range of values. We will therefore only apply it for large  $N$  ( $> 100$ ). The advantage of using it in this range is that it is more easily calculated than the upper bound in Eq. (67), whilst being significantly tighter than the bound on the error probability attained using Eq. (64).

## E. Upper bounds from PBT simulations

We now calculate the upper bounds based on PBT simulations of the AD channel. We consider three types of resource state, as mentioned in Subsection II B.

The first type is the Choi matrix of the simulated channels, resulting in the upper bounds in Ref. [25], which we call the

standard Choi bounds. These bounds are

$$D_{\mathcal{C}_X \mathcal{C}_Y}^{\text{opt}, N} \leq N \epsilon_{m, XY}^{\text{std}} + 2\sqrt{1 - f^{\text{Choi}}(\eta_X, \eta_Y)^{2mN}}, \quad (75)$$

$$\epsilon_m^{\text{std}}(\eta) = \xi_m \left( \frac{\eta}{2} + \sqrt{\eta} \right), \quad (76)$$

$$\epsilon_{m, XY}^{\text{std}} = \epsilon_m^{\text{std}}(\eta_X) + \epsilon_m^{\text{std}}(\eta_Y), \quad (77)$$

where  $m$  can take any positive, integer value. Note that we have a family of bounds, since we have a bound for any value of the number of ports,  $m$ . We must then optimise over  $m$  to achieve the tightest possible bound in this family.

The second type of resource state is similar to the first, but  $\eta_X$  and  $\eta_Y$  have been replaced by  $\eta'_X$  and  $\eta'_Y$ , according to Eq. (19). The reason we choose this value of  $\eta'_{X(Y)}$  is that this is one of the points at which the diamond norm between the channel and its simulation coincides with the trace norm. This means that we have an analytical expression for the resulting family of trace norm bounds, which we call the improved Choi bounds. Further, for all values of  $m \geq 6$ , the simulation errors are lower than for the standard Choi resource. These bounds are

$$D_{\mathcal{C}_X \mathcal{C}_Y}^{\text{opt}, N} \leq N \epsilon_{m, XY}^{\text{imp}} + 2\sqrt{1 - f^{\text{Choi}}(\eta'_X, \eta'_Y)^{2mN}}, \quad (78)$$

$$\epsilon_m^{\text{imp}}(\eta) = \frac{1}{2} \left( \frac{(\eta)\xi_m}{1 - \xi_m} + \sqrt{4(\eta) \left( 1 - \sqrt{1 - \xi_m} \right)^2 + \frac{\eta^2 \xi_m^2}{(1 - \xi_m)^2}} \right), \quad (79)$$

$$\epsilon_{m, XY}^{\text{imp}} = \epsilon_m^{\text{imp}}(\eta_X) + \epsilon_m^{\text{imp}}(\eta_Y). \quad (80)$$

In fact, since the chosen values of  $\eta'_X$  and  $\eta'_Y$  are not necessarily the values that give the tightest possible bounds, we could numerically minimise over all pairs of ‘‘Choi-like’’ resources simulating  $\mathcal{C}_X$  and  $\mathcal{C}_Y$ . In other words, we could simulate  $\mathcal{C}_X$  with  $R^{\text{Choi}}(\eta'_X)$  and  $\mathcal{C}_Y$  with  $R^{\text{Choi}}(\eta'_Y)$ , where

$$R^{\text{Choi}}(\eta) = C(\eta)^{\otimes m}, \quad (81)$$

$$C(\eta) = \begin{pmatrix} \frac{1-\eta}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{\sqrt{\eta}}{2} & 0 \\ 0 & -\frac{\sqrt{\eta}}{2} & \frac{\eta}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \quad (82)$$

Note that, in the context of ‘‘Choi-like’’ resources, the Bell pair used to generate the Choi state is the state  $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ . We could then numerically minimise over  $\eta'_X$  and  $\eta'_Y$  to find the optimal resource states. However, in this case, we would not have an analytical expression for the simulation error, and would need to calculate it numerically, by finding the diamond norm for both simulations; this involves maximising the trace norm between the channels and their simulations over all possible input states. We would then also need to minimise the bounds over  $m$ . This would involve a lot more numerical minimisation/maximisation than simply numerically optimising the standard and improved Choi bounds over  $m$ . This is why we do not find optimal bounds for this more general resource.

Finally, we consider resource states,  $R^{\text{alt}}(a)$ , of the form given in Eq. (20). The Choi matrix of the channel simulated by



carrying out PBT with this resource state is given in Ref. [42]. Writing the Choi matrix in the form

$$\rho_{\text{PBT}(R^{\text{alt}}(a))}^{\text{Choi}} = \begin{pmatrix} x & 0 & 0 & z \\ 0 & \frac{1}{2} - x & 0 & 0 \\ 0 & 0 & y & 0 \\ z & 0 & 0 & \frac{1}{2} - y \end{pmatrix}, \quad (83)$$

where the expressions for  $x$ ,  $y$  and  $z$  are functions of  $a$  (and  $m$ ), which are given in Ref. [42], we choose  $a_{X(Y)}$  such that

$$x(a_{X(Y)}) - y(a_{X(Y)}) = \frac{\eta_{X(Y)}}{2}. \quad (84)$$

We then simulate  $\mathcal{C}_{X(Y)}$  with  $a_{X(Y)}$ , and call the resulting bounds the alternative resource bounds. We choose this value of  $a_{X(Y)}$  because this is one of the points at which the diamond norm between the channel and its simulation coincides with the trace norm. Similarly to the case of the ‘‘Choi-like’’ resources, we could minimise our bound over all possible values of  $a_{X(Y)}$ , rather than choosing this value, but this would again require a lot more numerical minimisation/maximisation. The simulation error is given by

$$\epsilon^{\text{alt}}(a_{X(Y)}) = 1 - \eta_{X(Y)} - 2y + \sqrt{(1 - \eta_{X(Y)} - 2y)^2 + (\sqrt{\eta_{X(Y)}} - 2z)^2} \Big|_{a=a_{X(Y)}}, \quad (85)$$

and the fidelity between the resource states is given by

$$f^{\text{alt}}(a_X, a_Y) = \sqrt{a_X a_Y} + \sqrt{(1 - a_X)(1 - a_Y)}. \quad (86)$$

The alternative resource bounds are therefore given by

$$D_{\mathcal{C}_X \mathcal{C}_Y}^{\text{opt}, N} \leq N \epsilon_{XY}^{\text{alt}} + 2\sqrt{1 - f^{\text{alt}}(a_X, a_Y)^{2mN}}, \quad (87)$$

$$\epsilon_{XY}^{\text{alt}} = \epsilon^{\text{alt}}(a_X) + \epsilon^{\text{alt}}(a_Y). \quad (88)$$

Although this may not be immediately apparent from the expressions, both  $\epsilon_{XY}^{\text{alt}}$  and  $f^{\text{alt}}$  depend on  $m$ , since the expressions for  $x$ ,  $y$ ,  $z$  and  $a_{X(Y)}$  all depend on  $m$ . Therefore, we again want to pick the optimal value of  $m$ , in order to achieve the tightest possible bound. Note that the resource states are pure, meaning that our expression for the trace norm between different resource states is exact.

In order to optimise over  $m$ , we use analytical functions that closely approximate the standard and improved Choi bounds, but that do not feature  $\xi_m$ . This is done because the expression for  $\xi_m$  is too complicated to easily find an analytical minimum of the full bounds. Specifically, we replace  $\xi_m$  in the simulation error expressions with  $m^{-1}$ ; this gives us expressions that we can easily locate the minima of, for fixed  $\eta_X$ ,  $\eta_Y$  and  $N$ . We then use the closest integer values of  $m$  to our minima when calculating the actual values of the bounds (substituting them into the original expressions). When referring to the standard or improved Choi bound in Section III, it is implicit that this process has been carried out, and that the bounds are calculated for the optimal value of  $m$ . For the alternative resource bounds, we find numerically that the bound gets tighter as  $m$  increases, rather than having a maximum, so we pick a fixed, high value of  $m$ .

## G. Extending to the qudit case

We will briefly consider the case in which we must discriminate between two pure loss, qudit channels, rather than two AD channels (which are pure loss, qubit channels). The Stinespring dilation of such a channel is a beamsplitter acting on an environmental vacuum mode. The action of the beamsplitter can be described as

$$|n\rangle_S |0\rangle_E \rightarrow \sum_{i=0}^n \sqrt{\eta^{n-i}(1-\eta)^i} \binom{n}{i} |n-i\rangle_S |i\rangle_E, \quad (89)$$

where  $S$  labels the signal mode (the input mode to the channel),  $E$  labels the environmental mode and  $\eta$  is the transmissivity of the beamsplitter (and the channel). The binomial coefficient on the right-hand side of the expression comes from the choice of which photons are transferred to the environmental modes. This means that a  $d$ -dimensional, pure loss channel, with transmissivity  $\eta$ , can be described by the  $d$  Kraus operators

$$K_j = \sum_{i=j}^{d-1} \sqrt{\eta^{i-j}(1-\eta)^j} \binom{i}{j} |i\rangle \langle i-j|, \quad (90)$$

where the label  $j$  ranges from 0 to  $d-1$ .

Calling our pure loss,  $d$ -dimensional channels  $\mathcal{C}_X^d$  and  $\mathcal{C}_Y^d$ , with transmissivities of  $\eta_X$  and  $\eta_Y$  respectively, the  $J$ -matrix of the two channels (the difference between the Choi matrices, multiplied by the input dimension of the channel, as per Subsection II D) can be written as

$$J(\mathcal{C}_X^d, \mathcal{C}_Y^d) = \sum_{i=0}^{d-1} (|v_{\eta_X}^i\rangle \langle v_{\eta_X}^i| - |v_{\eta_Y}^i\rangle \langle v_{\eta_Y}^i|)_{SI}, \quad (91)$$

$$|v_{\eta}^i\rangle_{SI} = \sum_{j=0}^{d-i-1} \sqrt{\eta^j(1-\eta)^i} \binom{i+1}{j} |i+j\rangle_S |j\rangle_I, \quad (92)$$

where  $S$  labels the signal mode and  $I$  labels the idler mode.

In order to calculate simulation bounds in the qudit case, we would require expressions for the output of qudit PBT channels, and would require new resource states capable of simulating pure loss, qudit channels. However, the trivial bound, based on the diamond norm, can still be used in the qudit case (substituting the diamond norm between channels  $\mathcal{C}_X$  and  $\mathcal{C}_Y$ , in Eq. (24), with the diamond norm between  $\mathcal{C}_X^d$  and  $\mathcal{C}_Y^d$ ).

We do not have an analytical expression for the diamond norm between channels  $\mathcal{C}_X^d$  and  $\mathcal{C}_Y^d$ , as we do for the qubit case. Instead, we can find it numerically, using semidefinite programming, using the formula for the difference between Choi matrices, given in Eq. (91). The issue here is the same as with finding the diamond norm for multiple channel uses. As the input dimension becomes large (i.e. for large  $d$ ), numerically finding the diamond norm becomes computationally expensive. An alternative is to bound the diamond norm, using a result from Ref. [46].

Ref. [46] showed that the diamond distance between any two channels,  $\mathcal{A}$  and  $\mathcal{B}$ , can be bounded by

$$\|\mathcal{A} - \mathcal{B}\|_{\diamond} \leq \|\text{Tr}_S |J(\mathcal{A}, \mathcal{B})|\|_{\infty}, \quad (93)$$

where  $J(\mathcal{A}, \mathcal{B})$  is the difference between the Choi matrices of  $\mathcal{A}$  and  $\mathcal{B}$ , multiplied by the input dimension of the channels. Here we have first taken the absolute value of the matrix  $J(\mathcal{A}, \mathcal{B})$ , then taken the partial trace over the signal mode. We have then taken the largest eigenvalue (the operator norm) of the resulting matrix as our bound. Note that this coincides with the trace norm, and is therefore exactly the diamond distance, if the matrix is scalar after the partial trace is taken. Applying this bound to the expression in Eq. (91) gives a computationally cheaper (but less tight) bound on the diamond norm (and hence on the optimal trace distance between protocol outputs) than finding the diamond norm numerically, via semidefinite programming.

Numerical investigation shows that the diamond norm between two qudit channels,  $\mathcal{C}_X^d$  and  $\mathcal{C}_Y^d$ , appears to coincide with the diamond norm between  $d-1$  uses of two qubit channels,  $\mathcal{C}_X^{\otimes d-1}$  and  $\mathcal{C}_Y^{\otimes d-1}$  (for the same transmissivities,  $\eta_X$  and  $\eta_Y$ ). This suggests some connection between the two cases, however it is not clear what the connection is.

It is also worth noting that the (approximation of the) upper bound on the error probability of discriminating between two equiprobable channels attained by using the QCRB still holds in the qudit case (as long as the number of channels is large enough for the approximation to be valid), with the only change being to the lower bound on the channel parameter variance, in Eq. (70). In this equation,  $N(d-1)$  is substituted for  $N$ . This is because the maximum QFI per channel use is

$$H_{\eta,d}^{\max} = \frac{d-1}{\eta(1-\eta)}, \quad (94)$$

and the input state that attains this value is  $|d-1\rangle$  [35, 44]. The QFI is additive, so the maximum value of the total QFI is the same for both lossy channels and AD channels, as long as the total number of photons sent through the channel is the same.

### III. NUMERICAL INVESTIGATIONS

Carrying out numerical PBT simulations for our three classes of resource states over a variety of  $\eta_X$ ,  $\eta_Y$  and  $N$  values, we find that the improved Choi bound beats the standard Choi bound over the entire range of investigated parameter values. We also find that the alternative resource bound, for a sufficiently large number of ports,  $m$ , beats the both Choi bounds across almost the entire range, and that the trivial bound also beats the Choi bounds over a wide range of values. In fact, either the trivial bound or the alternative resource bound beat both of the Choi bounds over the entire range of values that was investigated. Since this was a numerical study, it is not possible to definitively say that the tightest out of the trivial bound and the alternative resource bound is always tighter than either of the Choi bounds, however this is the case for a wide range of parameter values.

In Figs. 1 and 2, we demonstrate the performance of the various bounds. Choosing  $\eta_X > \eta_Y$ , we decompose  $\mathcal{C}_Y$  as the pointwise application of  $\mathcal{C}_X$  and some other AD channel,

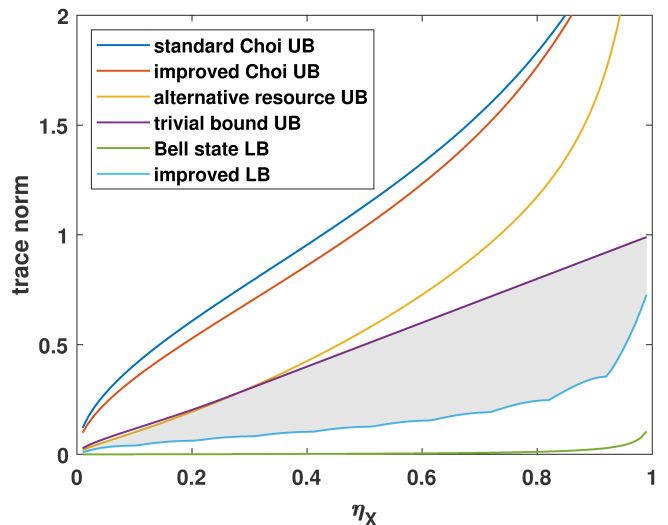


Figure 1. Upper and lower bounds on the maximum value of the trace norm between the two possible outputs of an adaptive discrimination protocol with no more than 10 channel uses. The channels being discriminated between are AD channels with transmissivities  $\eta_X$  and  $\eta_Y$ , where  $\eta_Y = \eta_X \eta_{XY}$ . In this case,  $\eta_{XY} = 0.95$ . The two upper bounds based on PBT simulations using “Choi-like” resources are significantly less tight than the trivial (upper) bound and the upper bound based on PBT simulations using the alternative resource. Each of these latter two bounds is optimal over some range of  $\eta_X$  values. The improved lower bound is tighter than the Bell state lower bound. The grey shaded area is the region between the tightest upper and lower bounds.

$\mathcal{C}_{XY}$ , with transmissivity

$$\eta_{XY} = \frac{\eta_Y}{\eta_X}. \quad (95)$$

Two specific values of  $\eta_{XY}$  (one per plot) were chosen: 0.95 and 0.9. Two values of  $N$ , the total number of channel uses, were also chosen: 10 and 30. With these kept fixed,  $\eta_X$  was then varied from 0.01 to 0.99 and the bounds were studied over this range. For the alternative resource bound, we have set  $m = 150$ .

As shown in the plots, the improved Choi bound performs better than the standard Choi bound, however both are beaten by either the trivial bound or the alternative resource bound (which of these is highest depends on the parameter values). The trivial bound performs better than the alternative resource bound when  $\eta_X$  and  $\eta_{XY}$  are large and when  $N$  is small.

Fig. 3 illustrates the  $N$ -dependence of the various trace norm bounds. In this plot,  $\eta_X = 0.75$  and  $\eta_{XY} = 0.9$ . The value of  $N$  is then varied from 0 to 20. The trivial bound (which is tight for  $N = 1$ ) is the tightest upper bound for low  $N$ , but is beaten by the alternative resource bound for  $N > 7$ , because the former scales linearly whilst the latter scales sub-linearly.

The new lower bound on the optimal trace distance (based on sending  $N$  copies of the state  $|1\rangle$  through the channel) is tighter than the lower bound from Ref. [25] (based on sending  $N$  copies of a Bell state through the channel) across the entire

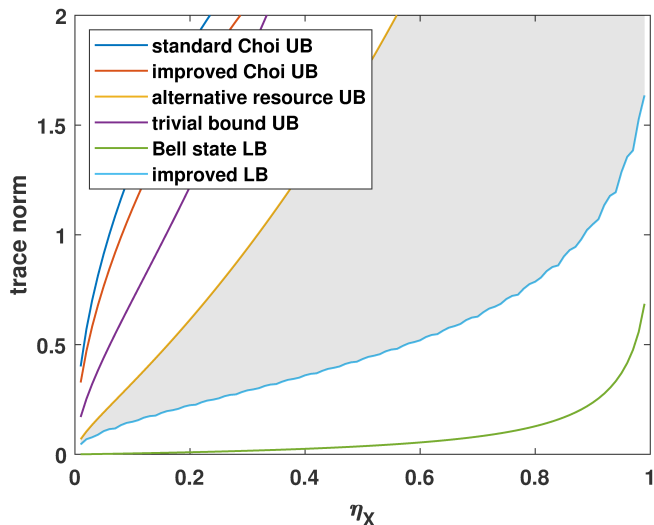


Figure 2. Upper and lower bounds on the maximum value of the trace norm between the two possible outputs of an adaptive discrimination protocol with no more than 30 channel uses. The channels being discriminated between are AD channels with transmissivities  $\eta_X$  and  $\eta_Y$ , where  $\eta_Y = \eta_X \eta_{XY}$ . In this case,  $\eta_{XY} = 0.9$ . For these parameter values, the upper bound based on simulation using the alternative resource is always better than the other three upper bounds. It is to be expected that the trivial bound performs less well for high values of  $N$ , because it scales linearly with  $N$ , whilst the bounds based on PBT do not. The improved lower bound has a distinct advantage over the Bell state lower bound. The grey shaded area is the region between the tightest upper and lower bounds.

range. It is clear, however, that there is still room to tighten either the upper or the lower bounds, since there is still a gap between the tightest upper bound and the tightest lower bound, especially in Fig. 2.

In Fig. 4, we compare our new bounds to the bounds presented in Fig. 4 of Ref. [25]. We plot the error probability of discriminating between two AD channels, with equal prior probability, using the equation in Eq. (18). The AD channels are characterised by the damping rate,  $p$ , rather than by the transmittance,  $\eta$ , although the two quantities are trivially connected via the equation  $p = 1 - \eta$ . One channel has a damping rate of  $p$  and the other has a damping rate of  $p + 0.01$ . The maximum number of channel uses is 20. The new lower bounds on the error probability (which come from the new upper bounds on the trace norm) are tighter than the lower bounds in Ref. [25] over the entire range; in this case, the alternative resource bound is the tightest lower bound. The new upper bound on the error probability (coming from the improved lower bound on the optimal trace norm) is slightly tighter than the upper bound in Ref. [25] over the entire range, but most noticeably for a high damping rate,  $p$ .

We now consider two examples of how these bounds might be applied to quantum information tasks. The tasks we consider are quantum hacking and biological sensing (a quantum metrology task).

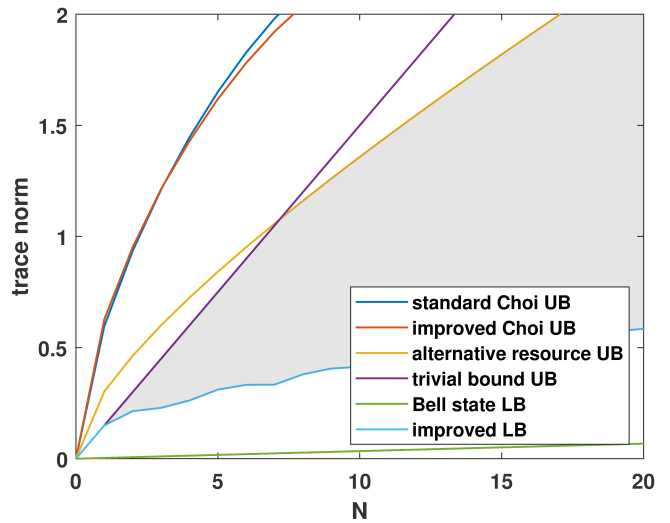


Figure 3. Upper and lower bounds on the maximum value of the trace norm between the two possible outputs of an adaptive discrimination protocol for varying numbers of channel uses. The channels being discriminated between are AD channels with transmissivities  $\eta_X = 0.75$  and  $\eta_Y = 0.675$ . For low  $N$ , the trivial bound is the tightest upper bound, whilst for  $N > 7$ , the alternative resource bound is the tightest upper bound. The grey shaded area is the region between the tightest upper and lower bounds.

### A. Applying the bounds to quantum hacking

Suppose a hacker, Eve, is attempting to eavesdrop on communications between a sender, Alice, and a receiver, Bob, who are implementing the BB84 protocol. Suppose also that Eve is able to send photons into Alice's device before each transmission (and to receive some return state). Eve could use this side-channel to gain more information on the states sent by Alice than is accounted for in the security proofs. For instance, Alice's basis choice could be enacted by a polariser [47]. By sending in photons with a known polarisation, Eve could glean information about Alice's basis choice based on the loss experienced by the photons (which could be basis dependent). Then, if Eve could determine Alice's basis with a high probability of success, she could carry out an intercept and resend attack on the photons sent through the main channel, without greatly disturbing them. In other words, she could measure the signal states in the basis that she believes them to have been sent in, based on her side-channel attack. Alice and Bob would only detect errors in half of the cases in which Eve incorrectly guesses Alice's basis. Since, in this scenario, Eve's error probability is low, the quantum bit error rate (QBER) detected by the trusted parties would be much lower than the 25% normally expected for an intercept and resend attack.

We model the attack as Eve carrying out a general, adaptive discrimination protocol with up to  $N$  channel uses. We set the transmissivity of one of the channels as  $\eta_Y = 0$ , and then choose three different values of  $\eta_X$ :  $10^{-5}$ ,  $5 \times 10^{-6}$  and  $10^{-6}$ . We then calculate Eve's discrimination error probability, assuming equal prior probabilities of each channel occur-

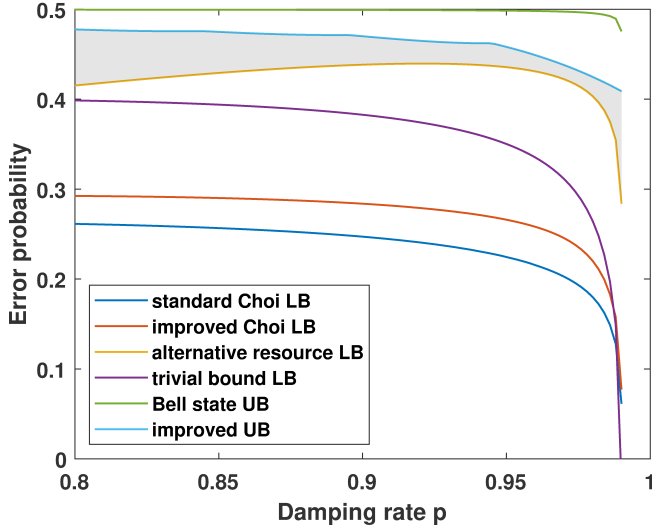


Figure 4. Comparison with the bounds on the error probability of discriminating between two AD channels, one with damping rate  $p$  and one with damping rate  $p + 0.01$ , with equal prior probabilities, with no more than 20 channel uses, found in Ref. [25]. The line labelled “standard Choi” is the lower bound found in Ref. [25], and the line labelled “Bell state UB” is the upper bound from the same paper. The other lines are the new bounds presented here, and the grey shaded area is the region between the tightest upper and lower bounds.

ring, for various numbers of channel uses. In this scenario, we assume that we have a perfect polariser, and so for one channel (i.e. for one polarisation), the photons sent through are completely absorbed by the polariser, whilst for the other channel, they are undisturbed by the polariser. We assume that the input states are so strongly attenuated that they can be modelled as a train of at most single photon states by the time they arrive at the polariser, and hence that Eve’s protocol can be modelled as a discrimination protocol between AD channels. This is a reasonable assumption, since BB84 involves the sending of single-photon states, which are often produced using strongly attenuated laser pulses. It is thus reasonable to assume that a laser pulse sent by Eve into Alice’s device, through the optical fibre, would be similarly attenuated, such that the pulse arriving at the polariser could be well-modelled as a qubit state. We also assume that further attenuation occurs as the states leave the device, giving rise to the low values of  $\eta_X$ . This is in line with the architecture in Ref. [48], which limits the total mean photon number leaving Alice’s device via the optical fibre, per signal sent through the main channel, to  $10^{-6}$ .

The assumption that Eve’s states can be modelled as (up to) one-photon states probing AD channels can be justified by numerically finding the energy-constrained diamond norm [24, 49, 50] between a lossy channel and the pointwise application of a truncation channel (a channel mapping all number states of the form  $|n > 1\rangle$  to  $|0\rangle$ ) and the same lossy channel, for low transmissivities. More specifically, we use the semidefinite programme for calculating the energy-constrained diamond norm given in Ref. [50]; note that the

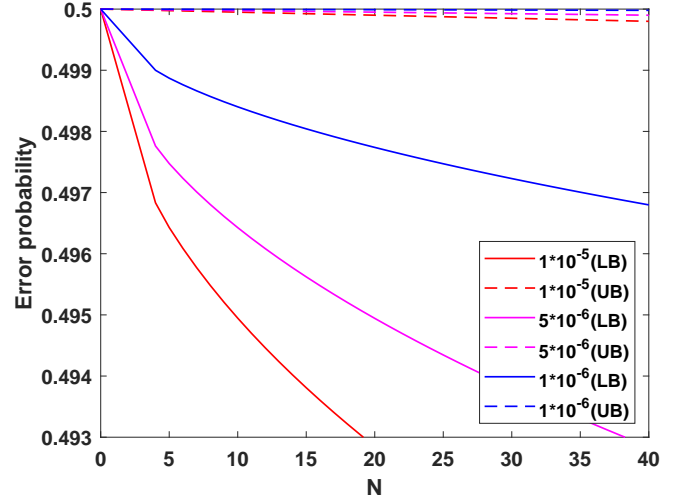


Figure 5. Upper and lower bounds on the discrimination error probability for an eavesdropper carrying out an adaptive protocol to discriminate between two BB84 preparation bases, with at most  $N$  channel uses. We assume that Eve must send qubit states through an AD channel, in order to determine whether the channel has a transmissivity of  $\eta_X$  or of  $\eta_Y$ .  $\eta_Y = 0$ , whilst  $\eta_X$  takes values of  $10^{-5}$ ,  $5 \times 10^{-6}$  and  $10^{-6}$ ; each case is represented by a different colour. The continuous lines give lower bounds on the error probability, whilst the dashed lines give upper bounds. The upper bounds are based on the improved lower bound, from Eq. (67). The lower bounds are based on the trivial bound, from Eq. (24), and the alternative resource bound, from Eq. (88); whichever bound has a higher value for a given  $N$  is used for that value of  $N$ . For the alternative resource bound,  $m = 150$ . We find that, for all three values of  $\eta_X$ , the trivial bound gives a tighter bound for  $N \leq 4$  and the alternative resource bound gives a tighter bound for  $N > 4$ .

definition of the energy-constrained diamond norm used by Ref. [50] (and Ref. [49]) differs slightly from the definition given by Ref. [24]. We find that, for  $\eta_X = 10^{-6}$ , the truncation to one-photon states has a small effect on the error probability. See the Supplementary data for further details [51].

Since one of the channels ( $C_Y$ ) will always output the state  $|0\rangle$ , we can significantly simplify the improved lower bound. Eq. (67) reduces to

$$D_{C_X C_Y}^{[1], N} = 2(1 - \eta_X^N). \quad (96)$$

The upper and lower bounds found are shown in Fig. 5. The upper bounds come from the improved lower bound and the lower bounds are based on whichever is tighter of the trivial bound and the alternative resource bound. For the chosen values of  $\eta_X$ , the trivial bound is tighter for  $N \leq 4$ . This is in line with our expectation that the trivial bound performs less well (compared to bounds based on PBT simulation) for large values of  $N$ , due to its linear scaling. The gap between the upper and lower bounds is small in proportion to their values, but still shows significant room for improvement, especially for large  $N$ . It is not clear whether it is the upper bounds, the lower bounds, or both which need tightening.

## B. Applying the bounds to biological sensing

Quantum channel discrimination protocols have applications in biology. The concentration of bacteria in a growth medium affects the transmissivity of light through the medium. The tasks of distinguishing between the presence and absence of bacteria in a sample and of distinguishing between two possible concentrations of bacteria can therefore be considered to be quantum channel discrimination tasks, where the two possible channels are lossy channels with different transmissivities. Further, in biological applications, low photon numbers are often desirable, since intense radiation can harm the samples that are being probed. As a result, in some scenarios, modelling the task as an AD channel discrimination task may be appropriate.

In Ref. [35], the authors showed that quantum light sources and detectors can reduce the error probability for both detecting the presence or absence of *E. coli* in a sample and determining whether a sample contains *E. coli* or *Salmonella*. They started by determining the transmissivities of growth media containing *E. coli* and *Salmonella* bacteria, as a function of time. The time-dependence comes from the changing concentrations of the bacteria in the media as they grow. The two possible types of bacteria and the case with no bacteria present therefore correspond to three different possible lossy channels. Determining whether a specific bacteria is present or absent and determining which of the two types of bacteria is present then become channel discrimination tasks.

Ref. [35] considers the task of parameter estimation, where the parameter to be estimated is the transmissivity of the channel. It considers both coherent state sources and the optimal input states for parameter estimation from Ref. [44] (which are number states that send the maximum number of photons through the channel per channel use). It then bounds the error probability for detecting the presence of *E. coli* and discriminating between *E. coli* and *Salmonella*, by using the expressions in Eqs. (72) and (73). In the symmetric testing case (equal prior probabilities), the mean of  $p_X^{\text{err}}$  and  $p_Y^{\text{err}}$  is minimised over  $\tau$ . Note, however, that the resulting expression (the QCRB bound) only provides an upper bound on the optimal error probability for sufficiently large  $N$  (i.e. in the regime in which the QCRB is tight).

In Figs. 6 and 7, we plot upper and lower bounds on the optimal error probability for an adaptive protocol with up to 150 channel uses, each sending at most one photon through the channel. This is reasonable, because it is desirable to send only a small amount of energy through the channels and because the error probabilities from Eqs. (72) and (73) can be achieved in this way.

Fig. 6 bounds the error probability over time for detecting the presence of *E. coli* in a sample. In this scenario,  $C_X$  is the channel corresponding to a blank sample (no bacteria present), and so  $\eta_X$  has a constant value of  $\eta_{\text{bk}} = 0.92$ .  $C_Y$  is the channel corresponding to a sample with *E. coli* present, and has a transmissivity of

$$\eta_Y = \eta_{E.Coli}(t) = \eta_{\text{bk}} - c_{1,E.Coli}t^2 + c_{2,E.Coli}t^3, \quad (97)$$

where  $c_{1,E.Coli}$  and  $c_{2,E.Coli}$  are constants with values of

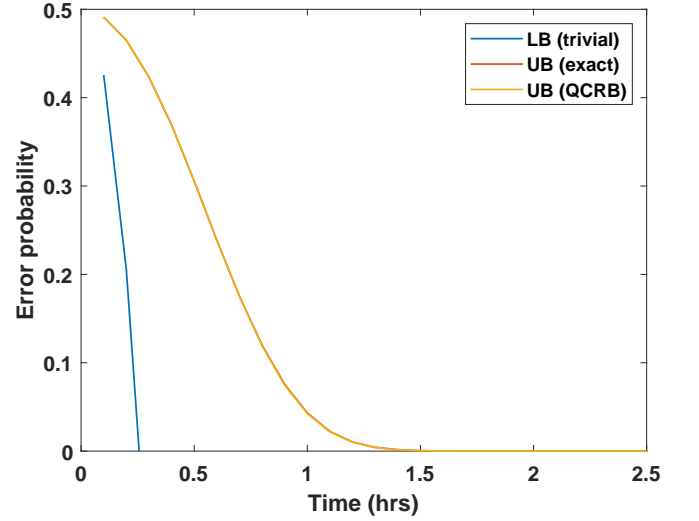


Figure 6. Upper and lower bounds on the error probability of detecting the presence of *E. Coli* bacteria in a sample, with a maximum of 150 channel uses (each using no more than one photon) as a function of time. The transmissivity of the blank sample is constant, whilst the transmissivity of the sample containing *E. Coli* is modelled as following a cubic equation (with respect to the time since the sample was prepared). The lower bound (denoted “LB (trivial)”) is derived from the trivial bound on the trace norm. The exact form of the upper bound (“UB (exact)”) is derived from the improved lower bound on the trace norm and the approximation to the upper bound (“UB (QCRB)”) is based on the QCRB bound. Since the two bounds overlap almost perfectly, the approximation is valid in this regime.

0.1 hrs<sup>-2</sup> and 0.0088 hrs<sup>-3</sup> respectively and where  $t$  is the time, in hours, since the sample was prepared. The values of  $c_{1,E.Coli}$  and  $c_{2,E.Coli}$  were experimentally determined in Ref. [35], and the cubic expression for  $\eta_{E.Coli}$ , from Eq. (97) is valid for small  $t$  ( $\leq 3$ ).

The lower bound is the tightest out of the lower bounds derived from our upper bounds on the trace norm. In fact, this is always the bound based on the trivial bound (in the regime in which the lower bound is  $> 0$ ). For the upper bound, we consider both the error probability derived from the exact form of the improved lower bound on the trace norm [from Eq. (67)] and the QCRB bound. Since the two bounds overlap almost perfectly, the approximation is valid in this regime ( $N = 150$ ). It is clear that there is room for improvement of either the upper or the lower bounds on the trace norm for large  $N$ .

Fig. 7 bounds the error probability over time for discriminating between samples of *E. coli* and *Salmonella*. In this scenario,  $C_X$  is the channel corresponding to a sample containing *E. coli* and  $C_Y$  is the channel corresponding to a sample containing *Salmonella*. In this case, we calculate the time-dependent transmissivities differently, by modelling the absorbances,  $A$ , of the samples as Gompertz functions and applying the formula

$$\eta = 10^{-A}. \quad (98)$$

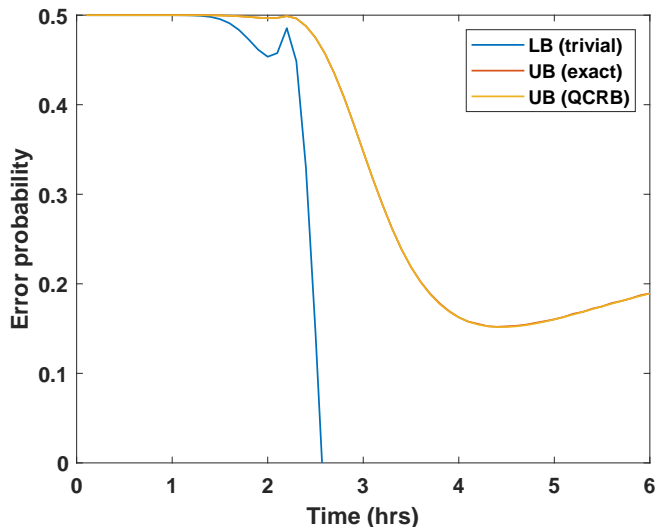


Figure 7. Upper and lower bounds on the error probability of discriminating between *E. Coli* and *Salmonella* bacteria in a sample, with a maximum of 150 channel uses (each using no more than one photon) as a function of time. The absorbances of the samples are modelled as following Gompertz functions. The lower bound (denoted “LB (trivial)”) is derived from the trivial bound on the trace norm. The exact form of the upper bound (“UB (exact)”) is derived from the improved lower bound on the trace norm and the approximation to the upper bound (“UB (QCRB)”) is based on the QCRB bound. Since the two bounds overlap almost perfectly, the approximation is valid in this regime. The absorbances are initially very similar, but become more distinguishable as the time since the sample was prepared increases. We note that this plot differs from Fig. 10 in Ref. [35]; this is because Ref. [35] considers probing with a mean total of  $10^3$  photons, whilst we only allow a maximum of 150 photons in total. Ref. [35] also models the transmissivities of the two samples using cubic equations, rather than Gompertz functions.

The absorbances are modelled as following

$$A = c_1 e^a + A_{bk}, \quad (99)$$

$$a = -e^{\frac{c_2 e}{c_1} (c_3 - t) + 1}, \quad (100)$$

where  $A_{bk}$  is the absorbance of a blank sample and  $c_1$ ,  $c_2$  and  $c_3$  are experimentally determined coefficients that depend on the type of bacteria present in the sample. Ref. [35] found that the triple  $(c_1, c_2, c_3)$  took values  $(0.309, 0.139, 2.634)$  for *E. coli* and  $(0.242, 0.0882, 2.672)$  for *Salmonella*.  $A_{bk}$  (which was the same for both samples) took the value 0.144.

The lower bound is derived from the tightest of our upper bounds on the trace norm, which is again the trivial bound over the entire regime in which the lower bound is  $> 0$ . The upper bounds are calculated in the same way as for Fig. 6, and

we again find that the exact form of the bound and the approximation overlap almost perfectly. The bounds briefly peak after a little more than 2 hours, before decreasing again, due to the fact that the difference in the absorbances of the samples briefly decreases before increasing again. Once again, we have a large gap between the bounds, which could be improved by tightening either the lower or the upper bounds. It is not yet known which bound most needs to be tightened.

#### IV. CONCLUSION

In this paper, we have presented multiple new bounds on the optimal trace norm for discriminating between two AD channels. We have strengthened both the upper and the lower bounds on the optimal trace norm by presenting the improved Choi bounds, the alternative resource bounds, the trivial bound and the improved lower bound on the trace norm. We have also calculated the exact diamond norm between AD channels, thus obtaining the exact error probability for one-shot channel discrimination between any two AD channels, in analytical form.

The bounds were then numerically investigated, and we found that the either the alternative resource bound or the trivial bound gave the tightest lower bound over a wide range of parameter  $(\eta_X, \eta_Y$  and  $N)$  values. The bounds were applied to two different scenarios: quantum hacking of BB84 and biological quantum metrology (detecting and discriminating between bacteria in a sample). In the latter scenario, we also confirm that the QCRB bound is valid as an approximation of the discrimination error probability derived from the improved lower bound on the trace norm (and is therefore a valid upper bound on the error probability) for large  $N$  (in our case,  $N = 150$ ).

We briefly discussed how these results could be extended to pure loss, qudit channels, however this is an area that is open to more research, which could find bounds on the error probability of adaptive discrimination protocols between any two lossy channels. Another area for continued research is the further tightening of either the upper or the lower bounds on the optimal trace norm, since there is still room for improvement.

In conclusion, our work contributes to the theory of channel simulation of AD channels and significantly improves the bounds on the optimal error probabilities for adaptive discrimination protocols between AD channels.

**Acknowledgments.** This work has been sponsored by the European Union’s Horizon 2020 Research and Innovation Action under grant agreement No. 862644 (FET-OPEN project: Quantum readout techniques and technologies, QUARTET) and by the EPSRC via the Quantum Communications Hub (Grant Nos. EP/M013472/1 and EP/T001011/1).

[1] S. Pirandola, B. R. Bardhan, T. Gehring, C. Weedbrook, and S. Lloyd, *Advances in photonic quantum sensing*, Nat. Photon.

**12**, 724 (2018).

[2] V. Scarani, and C. Kurtsiefer, *The black paper of quantum cryp-*

- tography: Real implementation problems, *Theor. Comput. Sci.* **560**, 27 (2014).
- [3] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, *Attacks on practical quantum key distribution systems (and how to prevent them)*, *Contemp. Phys.* **57**, 366 (2016).
- [4] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, *Advances in Quantum Cryptography*, arXiv:1906.01645 (2019).
- [5] C. W. Helstrom, *Quantum detection and estimation theory*, *J. Stat. Phys.* **1**, 231 (1969).
- [6] S. Lloyd, *Enhanced Sensitivity of Photodetection via Quantum Illumination*, *Science* **321**, 1463 (2008).
- [7] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, *Quantum Illumination with Gaussian States*, *Phys. Rev. Lett.* **101**, 253601 (2008).
- [8] J. H. Shapiro and S. Lloyd, *Quantum illumination versus coherent-state target detection*, *New J. Phys.* **11**, 063045 (2009).
- [9] S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola, *Microwave Quantum Illumination*, *Phys. Rev. Lett.* **114**, 080503 (2015).
- [10] Q. Zhuang, Z. Zhang, and J. H. Shapiro, *Entanglement-enhanced Neyman-Pearson target detection using quantum illumination*, *J. Opt. Soc. Am. B* **34**, 1567 (2017).
- [11] Q. Zhuang, Z. Zhang, and J. H. Shapiro, *Quantum illumination for enhanced detection of Rayleigh-fading targets*, *Phys. Rev. A* **96**, 020302(R) (2017).
- [12] M. M. Wilde, M. Tomamichel, S. Lloyd, and M. Berta, *Gaussian hypothesis testing and quantum illumination*, *Phys. Rev. Lett.* **119**, 120501 (2017).
- [13] Q. Zhuang, Z. Zhang, and J. H. Shapiro, *Entanglement-enhanced lidars for simultaneous range and velocity measurements*, *Phys. Rev. A* **96**, 040304(R) (2017).
- [14] G. De Palma and J. Borregaard, *Minimum error probability of quantum illumination*, *Phys. Rev. A* **98**, 012101 (2018).
- [15] R. Nair and M. Gu, *Fundamental limits of quantum illumination*, *Optica* **7**, 771 (2020).
- [16] A. Karsa, G. Spedalieri, Q. Zhuang, and S. Pirandola, *Quantum illumination with a generic Gaussian source*, *Phys. Rev. Res.* **2**, 023414 (2020).
- [17] E. D. Lopaeva, I. Ruo Berchera, I. P. Degiovanni, S. Olivares, G. Brida, and M. Genovese, *Experimental realization of quantum illumination*, *Phys. Rev. Lett.* **110**, 153603 (2013).
- [18] Z. Zhang, M. Tengner, T. Zhong, F. N. C. Wong, and J. H. Shapiro, *Entanglement's benefit survives an entanglement-breaking channel*, *Phys. Rev. Lett.* **111**, 010501 (2013).
- [19] Z. Zhang, S. Mouradian, F. N. C. Wong, and J. H. Shapiro, *Entanglement-enhanced sensing in a lossy and noisy environment*, *Phys. Rev. Lett.* **114**, 110506 (2015).
- [20] S. Pirandola, *Quantum reading of a classical digital memory*, *Phys. Rev. Lett.* **106**, 090504 (2011).
- [21] A. W. Harrow, A. Hassidim, D. W. Leung, and J. Watrous, *Adaptive versus nonadaptive strategies for quantum channel discrimination*, *Phys. Rev. A* **81**, 032339 (2010).
- [22] A. Acín, *Statistical Distinguishability between Unitary Operations*, *Phys. Rev. Lett.* **87**, 177901 (2001).
- [23] M. Hayashi, *Discrimination of Two Channels by Adaptive Methods and Its Application to Quantum System*, *IEEE Trans. Inf. Theory* **55**, 3807 (2009).
- [24] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Fundamental limits of repeaterless quantum communications*, *Nat. Commun.* **8**, 15043 (2017).
- [25] S. Pirandola, R. Laurenza, C. Lupo, and J. L. Pereira, *Fundamental limits to quantum channel discrimination*, *npj Quantum Inf.* **5**, 50 (2019).
- [26] T. P. W. Cope, L. Hetzel, L. Banchi, and S. Pirandola, *Simulation of non-Pauli channels*, *Phys. Rev. A* **96**, 022323 (2017).
- [27] S. Pirandola, R. Laurenza, and L. Banchi, *Conditional channel simulation*, *Ann. Phys. (N. Y.)* **400**, 289 (2019).
- [28] L. Banchi, J. Pereira, S. Lloyd, and S. Pirandola, *Convex optimization of programmable quantum computers*, *npj Quantum Inf.* **6**, 42 (2020).
- [29] S. L. Braunstein and C. M. Caves, *Statistical distance and the geometry of quantum states*, *Phys. Rev. Lett.* **72**, 3439 (1994).
- [30] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. (Cambridge University Press, USA, 2011).
- [31] S. Bose, *Quantum Communication through an Unmodulated Spin Chain*, *Phys. Rev. Lett.* **91**, 207901 (2003).
- [32] Q. Zhuang and S. Pirandola, *Ultimate Limits for Multiple Quantum Channel Discrimination*, *Phys. Rev. Lett.* **125**, 080505 (2020).
- [33] V. Katariya and M. Wilde, *Evaluating the Advantage of Adaptive Strategies for Quantum Channel Distinguishability*, arXiv:2001.05376 (2020).
- [34] M. Rexiti and S. Mancini, *Discriminating qubit amplitude damping channels*, arXiv:2009.01000 (2020).
- [35] G. Spedalieri, L. Piersimoni, O. Laurino, S. L. Braunstein, and S. Pirandola, *Detecting and tracking bacteria with quantum light*, *Phys. Rev. Res.* **2**, 043260 (2020).
- [36] K. M. R. Audenaert, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, Ll. Masanes, A. Acín, and F. Verstraete, *Discriminating States: The Quantum Chernoff Bound*, *Phys. Rev. Lett.* **98**, 160501 (2007).
- [37] J. Calsamiglia, R. Muñoz-Tapia, Ll. Masanes, A. Acín, and E. Bagan, *Quantum Chernoff bound as a measure of distinguishability between density matrices: Application to qubit and Gaussian states*, *Phys. Rev. A* **77**, 032311 (2008).
- [38] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [39] G. Bowen and S. Bose, *Teleportation as a Depolarizing Quantum Channel, Relative Entropy, and Classical Capacity*, *Phys. Rev. Lett.* **87**, 267901 (2001).
- [40] S. Ishizaka and T. Hiroshima, *Asymptotic Teleportation Scheme as a Universal Programmable Quantum Processor*, *Phys. Rev. Lett.* **101**, 240501 (2008).
- [41] S. Ishizaka and T. Hiroshima, *Quantum teleportation scheme by selecting one of multiple output ports*, *Phys. Rev. A* **79**, 042306 (2009).
- [42] J. Pereira, L. Banchi, and S. Pirandola, *Characterising port-based teleportation as a universal simulator of qubit channels*, arXiv:1912.10374 (2019).
- [43] J. Watrous, *Simpler semidefinite programs for completely bounded norms*, *Chicago Journal of Theoretical Computer Science* **2013** (2013).
- [44] G. Adesso, F. Dell'Anno, S. De Siena, F. Illuminati, and L. A. M. Souza, *Optimal estimation of losses at the ultimate quantum limit with non-Gaussian states*, *Phys. Rev. A* **79**, 040305(R) (2009).
- [45] S. L. Braunstein, A. S. Lane, and C. M. Caves, *Maximum-likelihood analysis of multiple quantum phase measurements*, *Phys. Rev. Lett.* **69**, 2153 (1992).
- [46] I. Nechita, Z. Puchała, Ł. Paweła, and K. Życzkowski, *Almost all quantum channels are equidistant*, *J. Math. Phys.* **59**,

- 052201 (2018).
- [47] Y. S. Kim, Y. C. Jeong, and Y. H. Kim, *Implementation of polarization-coded free-space BB84 quantum key distribution*, *Laser Phys.* **18**, 810 (2008).
  - [48] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, *Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution*, *Phys. Rev. X* **5**, 031030 (2015).
  - [49] M. E. Shirokov, *On the energy-constrained diamond norm and its application in quantum information theory*, *Probl. Inform. Transmiss.* **54**, 20 (2018).
  - [50] A. Winter, *Energy-constrained diamond norm with applications to the uniform continuity of continuous variable channel capacities*, arXiv:1712.10267 (2017).
  - [51] Supplementary data, including the code used for the various plots, is available at [doi.org/10.5281/zenodo.4281118](https://doi.org/10.5281/zenodo.4281118).