



Heriot-Watt University
Research Gateway

Benchmarking the state comparison amplifier

Citation for published version:

Kleczkowska, K, Puthoor, IV, Bain, L & Andersson, E 2017, 'Benchmarking the state comparison amplifier', *Physical Review A*, vol. 96, no. 4, 042309. <https://doi.org/10.1103/PhysRevA.96.042309>

Digital Object Identifier (DOI):

[10.1103/PhysRevA.96.042309](https://doi.org/10.1103/PhysRevA.96.042309)

Link:

[Link to publication record in Heriot-Watt Research Portal](#)

Document Version:

Publisher's PDF, also known as Version of record

Published In:

Physical Review A

Publisher Rights Statement:

©2017 American Physical Society. Kleczkowska, K., Puthoor, I. V., Bain, L., & Andersson, E. (2017). Benchmarking the state comparison amplifier. *Physical Review A*, 96(4), [042309]. DOI: 10.1103/PhysRevA.96.042309

General rights

Copyright for the publications made accessible via Heriot-Watt Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy

Heriot-Watt University has made every reasonable effort to ensure that the content in Heriot-Watt Research Portal complies with UK legislation. If you believe that the public display of this file breaches copyright please contact open.access@hw.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Benchmarking the state comparison amplifier

Klaudia Kleczkowska, Ittoop Vergheese Puthoor, Lauren Bain, and Erika Andersson

*Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University,
Edinburgh EH14 4AS, United Kingdom*

(Received 19 July 2017; published 9 October 2017)

The state comparison amplifier is a recently proposed probabilistic quantum amplifier, intended especially for amplifying coherent states. Its realization is simple and uses only linear optics and photodetectors, and the preparation of a “guess” state, typically a coherent state. Fidelity and success probability can be high compared with other probabilistic amplifiers. State comparison amplification does, however, extract information about the amplified state, which means that it is especially important to benchmark it against a simple measure-and-resend procedure. We compare state comparison quantum amplifiers to measure-and-resend strategies, and identify parameter regimes and scenarios where these can and where they cannot provide an advantage.

DOI: [10.1103/PhysRevA.96.042309](https://doi.org/10.1103/PhysRevA.96.042309)

I. INTRODUCTION

In both classical and quantum communication, one needs a way of overcoming loss. Quantum states cannot, however, be perfectly amplified. It is, for example, impossible to deterministically change an unknown coherent state $|\alpha\rangle$ into $|g\alpha\rangle$, where $g > 1$ is a gain factor. Imperfect quantum amplification, on the other hand, is possible. One option is heralded probabilistic quantum amplifiers, which do not always work, but when successful, they can amplify coherent states with relatively high fidelity. Ralph and Lund first suggested using “quantum scissors” [1] to realize heralded probabilistic amplification [2]. Subsequent proposals for heralded probabilistic amplifiers made use of photon addition and subtraction [3] and noise addition and subtraction [4,5]. Probabilistic amplifiers have also been realized, e.g., in Refs. [6–9], and their usefulness for quantum key distribution investigated [10–12]. One should note that probabilistic coherent-state amplifiers billed as “noiseless” usually are not noiseless in the sense that if the scheme is phase independent, the fidelity can only reach 100% for vanishing success probability [13]. However, for linearly independent coherent states, truly noiseless probabilistic amplification is actually possible [14].

Nevertheless, these probabilistic amplifiers are often non-trivial to realize, and the success probability is often prohibitively low if high fidelity is desired. Although the setup for “quantum scissors” [1] is based on linear optics, it requires single-photon auxiliary input states which are hard to prepare. The “quantum scissors” device truncates an incoming state to its zero- and one-photon components by an arrangement of two beam splitters and an additional single-photon resource state, conditioned on specific detection patterns in two of the output modes. It may seem counterintuitive that removing the contributions with higher photon numbers can result in amplification. As Ralph and Lund [2] show, however, for properly chosen beam-splitter coefficients, a large number of state truncation devices, operated successfully in parallel, results in the input state being approximately amplified. A single “scissors” device can probabilistically increase the amplitude of the single-photon component as compared with the amplitude of the zero-photon component, which for small initial coherent-state amplitude amounts to approximate amplification. Two-photon resource states in the “quantum scissors” device can somewhat improve the situation [15],

but this does not solve the issue of low success probability and having to generate nonclassical auxiliary states. Starting with [16,17] and an experimental realization in [18], the quantum scissors device has been the subject of a large body of subsequent work.

A recently introduced probabilistic quantum amplifier which in contrast is easier to realize is the state comparison amplifier (sometimes abbreviated SCAMP) [19,20]. Here, the state that is to be amplified is “compared” against a “guess state” by interference at a beam splitter. The success probability, gain, and fidelity can be relatively high, and the guess state can be a coherent state, which is easy to prepare. However, the success probability and fidelity do not necessarily tell us how useful an amplifier is in a practical scenario; further investigations are needed for this.

Since one obtains information about whether the input state is likely to have matched the guess state, one would expect the state comparison amplifier to be of limited use for amplifying entangled states. (One can, of course, in principle consider also entangled “guess” states, but this would render the amplifier much less practical.) Also, for the same reason, since the amplifier extracts information about the input state, it would likely have to be used in a secure node in a network for quantum cryptography, which somewhat limits its appeal. Especially since the amplifier is probabilistic, there are more effective ways to use secure nodes. Nevertheless, the state comparison amplifier is simpler than a setup for a full quantum key distribution node, and if it improves performance, it may be an alternative to consider.

It is therefore of interest to evaluate the usefulness of the state comparison amplifier. Because it extracts information about the state to be amplified, it is natural to benchmark it against simple measure-and-resend strategies. In particular, if the possible input states are drawn from a set of linearly independent quantum states, which is often the case in quantum communication and cryptography using coherent states of light, then it is possible to unambiguously distinguish between these with a finite probability of success [21]. A new perfectly “amplified” state can then be prepared with any gain, meaning that this type of amplification can be truly perfect with unlimited average gain [14]. Measure-and-resend strategies can also be used even if states are not drawn from a finite set of possible states. It makes more sense to use state

comparison amplification in parameter regimes and scenarios where its performance is in some respect better than that of a measure-and-resend strategy.

In this paper, we compare the state comparison amplifier to measure-and-resend strategies in terms of success probability and average fidelity, and when used in a lossy channel. In certain regimes, the success probability and average fidelity of state comparison amplifiers can beat those of measure-resend strategies. As for use in a lossy channel, we have been unable to find any regimes where a state comparison amplifier will increase the probability for the end receiver to distinguish between binary coherent states.

Measure-and-resend amplifiers, on the other hand, can increase the probability that a receiver at the end of a lossy channel will correctly infer what the original input state was, even when the allowed amplitude of the resent state, that is, the gain, is limited. However, this requires that the information on whether amplification was successful or not is sent along with the amplified state. Therefore, as one would expect, this type of amplifier in the considered scenario will not increase the classical information-carrying capacity of the communication channel. This still leaves the possibility that they could in principle be useful, e.g., as secure relay stations in a quantum communication network. However, measure-and-resend amplifiers turn out not to be useful for low-coherent-state amplitudes, and are therefore, even when used in secure nodes, less likely to be of practical relevance for quantum cryptography, which typically operates with weak coherent states. Again, there will be more efficient ways to use secure nodes in a quantum communication network.

The paper is organized as follows. First, in Sec. II, we review how the state comparison amplifier works, and in Sec. III, we review “amplification” using measure-and-resend strategies. In Sec. IV, we compare the performance of the state comparison amplifier and measure-and-resend strategies in terms of success probabilities and average fidelity. In Sec. V, we consider the use of both types of amplifier in a lossy communication channel.

II. STATE COMPARISON AMPLIFICATION

We first briefly review how state comparison amplification, introduced in Ref. [19], works. This amplifier would typically be used when the states to be amplified are selected at random from a known set of states. The input state (which is to be amplified) is compared against a “guess state” using the first beam splitter, *BS1*, in Fig. 1. If the input coherent state is $|\alpha\rangle$ and the guess state is $|\beta\rangle$, then this beam splitter transforms the combined state as

$$|\alpha\rangle_1 \otimes |\beta\rangle_2 \rightarrow |t_1\alpha - r_1\beta\rangle_1 \otimes |t_1\beta + r_1\alpha\rangle_2, \quad (1)$$

where the first output mode is directed onto detector *D1* and the second output mode continues to the second beam splitter, *BS2*. (Without loss of generality, all beam-splitter transmission and reflection coefficients are assumed to be real and positive.) If the guess state is chosen “correctly” as $|\beta\rangle = |t_1\alpha/r_1\rangle$, then this results in destructive interference (a vacuum state) in the first output mode, and detector *D1* will not fire. The coherent state in the second output mode is then

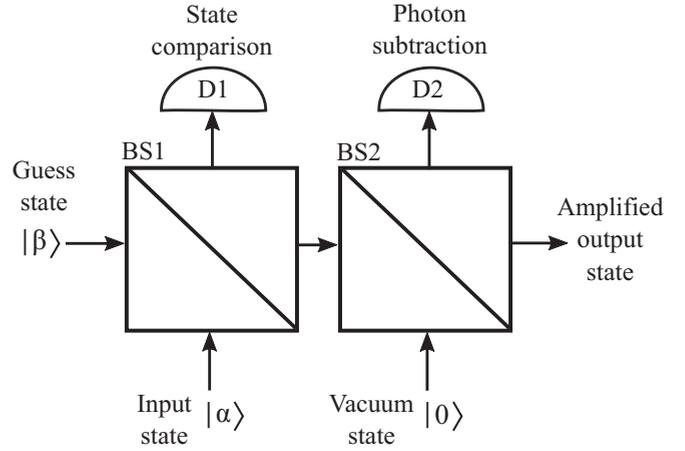


FIG. 1. The setup for the state comparison amplifier. The state to be amplified is interfered with a guess state on the first beam splitter, *BS1*, followed by photon subtraction at the second beam splitter, *BS2*. If detector *D2* fires, this increases the probability that the guess was right. Successful amplification of the input state occurs when no photons are detected by detector *D1* and detector *D2* does fire.

a coherent state $|\alpha/r_1\rangle$, which has a larger amplitude than the original state.

Let us, as in Ref. [19], consider the case when the input state is randomly selected either as $|\alpha\rangle$ or $|\alpha\rangle$. The guess state is drawn randomly as $|\beta\rangle = |\pm t_1\alpha/r_1\rangle$. Even when detector *D1* does not click, the guess might also have been wrong. Conditioned on detector *D1* not firing, the output state in output mode 2 of the first beam splitter will therefore be a mixed state. The confidence in the guess having been right can be increased using the second beam splitter, *BS2*, with transmission and reflection coefficients t_2 and r_2 . If the guess was right, then the total amplitude entering the second beam splitter is higher than if the guess was wrong, resulting in a higher probability for detector *D2* to fire if the guess is right; the amplitude in the output leading to *D2* is $r_2\alpha/r_1$ if the guess was correct and $r_2\alpha|t_1^2 - r_1^2|/r_1$ if it was incorrect. The amplified output amplitude is $t_2\alpha/r_1$ if the guess was correct, meaning that in this case, the gain $g = t_2/r_1$. If the guess was incorrect, then the output state has amplitude $t_2\alpha|t_1^2 - r_1^2|/r_1 = g\alpha|t_1^2 - r_1^2|$.

The amplification thus succeeds if detector *D1* does not fire and detector *D2* fires. In the scenario we are considering, with two possible input states, this gives a success probability of

$$p_s^{SC} = \frac{1}{2} \left\{ 1 - e^{-(\alpha/r_1)^2} + e^{-4(\alpha t_1)^2} \left[1 - e^{-(\alpha/r_1)^2(t_2^2 - r_1^2)^2} \right] \right\}, \quad (2)$$

or, in terms of only the gain g and t_2 , as given in the Supplemental Material of [19],

$$p_s^{SC} = \frac{1}{2} \left\{ 1 - e^{-(g\alpha)^2(1/t_2^2 - 1)} + e^{-4\alpha^2(1 - t_2^2/g^2)} \times \left[1 - e^{-(g\alpha)^2(1/t_2^2 - 1)(1 - 2t_2^2/g^2)} \right] \right\}. \quad (3)$$

If the detectors have efficiency η , then α^2 is replaced by $\eta\alpha^2$ in the above expressions.

The first term in the expression in curly brackets in the above expressions for p_s^{SC} give the probability that the guess is right and the amplification succeeds, which we will refer to

as the “true success probability,”

$$p_T^{SC} = \frac{1}{2} [1 - e^{-(\alpha r_2/r_1)^2}] = \frac{1}{2} [1 - e^{-(g\alpha)^2(1/t_2^2-1)}]. \quad (4)$$

The second term in the expressions for p_s^{SC} give the probability that the guess is incorrect and the amplification nevertheless “succeeds” (detector $D1$ does not fire and detector $D2$ fires), which we will refer to as the “false success probability,”

$$p_F^{SC} = \frac{1}{2} e^{-4(\alpha t_1)^2} [1 - e^{-(\alpha \frac{t_2}{r_1})^2(t_2^2-r_1^2)^2}] \\ = \frac{1}{2} e^{-4\alpha^2(1-t_2^2/g^2)} [1 - e^{-(g\alpha)^2(1/t_2^2-1)(1-2t_2^2/g^2)^2}]. \quad (5)$$

It holds that $p_T^{SC} + p_F^{SC} = p_s^{SC}$. These probabilities for “false” and “true” success will become relevant when benchmarking the state comparison amplifier. The “true” success probability is always higher than the “false” success probability, but they can become comparable to each other, in which case the confidence in the amplification having worked correctly is lower.

As a figure of merit, we will also be using an “average fidelity,” which is the success probability in Eq. (2), multiplied by the fidelity used in Ref. [19], which is the fidelity conditioned on success. This “average fidelity” is equal to $P(T,S)$ in Eq. (10) in the Supplemental Material of [19]. It is given by the “true” success probability times the square overlap of the desired and actual output states if the guess is correct (which is 1), plus the “false” success probability times the square overlap of the desired and actual output states if the guess is incorrect. If the input state is either $|\alpha\rangle$ or $|\alpha\rangle$, with equal probability, then the average fidelity is given by

$$F^{SC} = \frac{1}{2} \{1 - e^{-(\alpha \frac{t_2}{r_1})^2} + e^{-4(\alpha t_1)^2} [1 - e^{-(\alpha \frac{t_2}{r_1})^2(t_2^2-r_1^2)^2}]\}, \quad (6)$$

or, in terms of only g and t_2 ,

$$F^{SC} = \frac{1}{2} \{1 - e^{-(g\alpha)^2(1/t_2^2-1)} + e^{-4\alpha^2(1-t_2^2/g^2)} \\ \times [1 - e^{-(g\alpha)^2(1/t_2^2-1)(1-2t_2^2/g^2)^2}]\}. \quad (7)$$

One should keep in mind that a random guess will result in an average fidelity which is at least $1/2$. If the amplitude of the input state is small and the desired gain is moderate, the fidelity can approach 1 even for a random guess.

III. MEASURE-AND-RESEND FOR AMPLIFICATION

As in the previous section and as in [19], we consider the situation where the state to be amplified is either the coherent state $|\alpha\rangle$ or $|\alpha\rangle$, where the amplitude and phase of α are known; without loss of generality, we can assume α to be real and positive. These two states can be unambiguously distinguished with a finite success probability. That is, there is a measurement which sometimes fails, but when it succeeds, it correctly identifies the state. (Such an unambiguous measurement is possible whenever the states to be distinguished are linearly independent [21]. Any number of coherent states, in particular, the states $|\alpha\rangle$ and $|\alpha\rangle$, are linearly independent.)

Two equiprobable pure quantum states $|\psi_1\rangle$ and $|\psi_2\rangle$ can be unambiguously distinguished with an optimal success probability of $p_s = 1 - |\langle\psi_1|\psi_2\rangle|$ [22–24]. For the two coherent states $|\pm\alpha\rangle$ the optimal success probability therefore is

$$p_s^U = 1 - |\langle-\alpha|\alpha\rangle| = 1 - e^{-2\alpha^2}. \quad (8)$$

Although optimal generalized quantum measurements are by no means always easy to realize, in this case, the optimal measurement can be implemented by interfering the input state with a reference state on a balanced beam splitter [25]. A balanced beam splitter transforms two coherent states $|\alpha\rangle$ and $|\beta\rangle$ as

$$|\alpha\rangle \otimes |\beta\rangle \rightarrow |(\alpha + \beta)/\sqrt{2}\rangle \otimes |(\alpha - \beta)/\sqrt{2}\rangle \quad (9)$$

(modulo phase shifts on the input and output modes, which in this case are unimportant). If photons are detected in output port 1, then we can infer that $\alpha \neq -\beta$, and if photons are detected in output port 2, we can infer that $\alpha \neq \beta$. By interfering the state to be amplified $|\pm\alpha\rangle$ with a reference state $|\alpha\rangle$, we obtain

$$|\pm\alpha\rangle \otimes |\alpha\rangle \rightarrow |(\pm\alpha + \alpha)/\sqrt{2}\rangle \otimes |(\pm\alpha - \alpha)/\sqrt{2}\rangle \\ = \begin{cases} |\sqrt{2}\alpha\rangle \otimes |0\rangle & \text{for input state } |\alpha\rangle \\ |0\rangle \otimes |-\sqrt{2}\alpha\rangle & \text{for input state } |-\alpha\rangle. \end{cases} \quad (10)$$

No matter in what output mode photons are detected, we know for certain what the input state must have been. The measurement is unsuccessful if no photons are detected, which occurs with probability $\exp(-2\alpha^2)$. Hence the success probability is optimal for this realization. As an aside, it is also possible to distinguish between more than two coherent states using linear optics and photodetectors, but the success probability is not optimal [26].

If the unambiguous measurement succeeds, then we can prepare and resend a new copy of the state, $|\pm g\alpha\rangle$, with any desired gain and perfect fidelity. This way, a measure-and-resend strategy can serve as a probabilistic “amplifier” [14]. The measurement can be repeated at desired intervals and a new state resent. The gain is in principle unlimited but will in practice be limited. In Sec. V we will consider resending a state with the original amplitude when the amplitude of an input state has decreased in a lossy channel. This type of “amplification” obviously destroys any incoming superposition of the states $|\alpha\rangle$ and $|\alpha\rangle$, or any entanglement between the input state and some other state. Nevertheless, as we shall see, measure-and-resend strategies can increase the probability for a receiver at the end of a lossy channel to distinguish between the original states sent also when the amplitude of the resent state is limited.

Truly perfect amplification of a finite set of coherent states, for finite gain, is actually possible with somewhat higher success probability than an unambiguous measurement, which corresponds to the limit of infinite gain [14]. The optimal procedure for given finite gain is, however, not straightforward to implement. Since state comparison amplification is easily realizable, we will benchmark it against another easily realizable procedure, unambiguous state discrimination.

Also, if the possible input states are not linearly independent, then probabilistic measure-and-resend strategies cannot have perfect fidelity. Nevertheless, a measurement could still be used to obtain information about a quantum state and a new state resent. If wanting to benchmark the state comparison amplifier when the input states are linearly dependent, one could, for example, compare it to a maximum confidence

measurement [27], which maximizes the confidence in a result, given that a result is obtained.

IV. COMPARING SUCCESS PROBABILITIES AND FIDELITIES

A. Analytical results

“Measure-and-resend” allows for unlimited gain. We will therefore start by comparing the success probability of the state comparison amplifier, in the limit of large gain, to that of the unambiguous measurement. One would expect the state comparison to have a better chance of an advantage if the desired gain is moderate, but it is still instructive to consider the large-gain limit.

If $g = t_2/r_1$ becomes large, while α does not approach zero and t_2 does not approach 1 [the precise condition is that $g^2\alpha^2(1/t_2^2 - 1)$ should become large], then it holds for p_s^{SC} in Eq. (2) that

$$\lim_{g \rightarrow \infty} p_s^{SC} = \frac{1}{2}(1 + e^{-4\alpha^2}). \quad (11)$$

The success probability p_s^U in Eq. (8) is less than this limiting value if

$$\alpha^2 < -\frac{1}{2} \ln(\sqrt{2} - 1) \approx 0.44. \quad (12)$$

That is, if one is interested in large gain, it makes less sense to use a state comparison amplifier for α^2 larger than ~ 0.44 . If detectors have efficiency η , then the same bound applies, with α^2 replaced by $\eta\alpha^2$. For large α^2 , unambiguous state discrimination has a higher success probability and moreover gives perfect fidelity. For lower α^2 , the state comparison amplifier has a higher success probability, but we should remember that its fidelity will not be perfect. Before we can conclude that the state comparison amplifier can beat measure-and-resend for low α^2 , we will have to also look at the average fidelity.

Before doing so, let us also look at success probabilities when the gain is not necessarily large. When the state comparison amplifier succeeds, we cannot be certain that our guess was correct. It may be either correct or incorrect. Previously, we defined the probability of “true success” p_T^{SC} in Eq. (4). Now, if $p_T^{SC} < p_s^U$, again it makes less sense to use a state comparison amplifier; its total success probability may be greater than that of an unambiguous measurement, but the “true success” probability is not. In addition, we do not know when a success was a “true success” and the fidelity is imperfect.

To start with, we note that it always holds that $p_T^{SC} < 1/2$; this is the case because the guess state is randomly chosen. The unambiguous measurement succeeds with a probability larger than $1/2$ if $\alpha^2 > \frac{1}{2} \ln 2 \approx 0.35$, and in this case it makes less sense to use a state comparison amplifier. This bound, which now holds for any gain, is tighter than that obtained from the large-gain limit, partly because we are now taking into account only the “true” success probability. As we will see, for $\alpha^2 < \frac{1}{2} \ln 2$, it is possible to have $p_T^{SC} > p_s^U$ for certain choices of beam-splitter coefficients in the state comparison

amplifier. The condition $p_T^{SC} > p_s^U$, for any gain, reads

$$\frac{1}{2} \left[1 - e^{-\left(\alpha \frac{t_2}{t_1}\right)^2} \right] > 1 - e^{-2\alpha^2}, \quad (13)$$

and never holds when $\alpha^2 \geq \frac{1}{2} \ln 2$. When $\alpha^2 < \frac{1}{2} \ln 2$, then (13) can be rewritten as

$$r_2 > \frac{r_1}{\alpha} \sqrt{-\ln(2e^{-2\alpha^2} - 1)} = kr_1. \quad (14)$$

We are also only interested in regimes where the gain $g = t_2/r_1 > 1$. In terms of r_1 and r_2 , this second condition becomes $r_1^2 + r_2^2 < 1$.

The parameter region where the true success probability p_T^{SC} of the state comparison amplifier is larger than the success probability p_s^U for the unambiguous measurement is thus given by $\alpha^2 < \frac{1}{2} \ln 2$, and values (r_1, r_2) which lie both inside the circle $r_1^2 + r_2^2 < 1$ and above the line $r_2 = kr_1$, where k , defined in Eq. (14), depends only on α . The circle and the line intersect when

$$r_1^2 = \frac{\alpha^2}{\alpha^2 - \ln(2e^{-2\alpha^2} - 1)} = r_{1, \max}^2, \quad (15)$$

which gives the highest value of r_1 for which $p_T^{SC} > p_s^U$ is possible. When $\alpha^2 \rightarrow 0$, then $r_{1, \max} \rightarrow 1$, and when $\alpha^2 \rightarrow \frac{1}{2} \ln 2$, then $r_{1, \max} \rightarrow 0$. For α^2 and r_1 chosen such that $p_T^{SC} > p_s^U$ is possible, we must also choose r_2 so that

$$-\frac{r_1^2}{\alpha^2} \ln(2e^{-2\alpha^2} - 1) = r_{2, \min}^2 < r_2^2 < r_{2, \max}^2 = 1 - r_1^2. \quad (16)$$

We also note that for any gain g , it holds that $g^2 = t_2^2/r_1^2$, that is, $g^2 r_1^2 + r_2^2 = 1$. These curves are ellipses in the (r_1, r_2) plane, intersecting the r_1 axis at $r_1 = 1/g$ and the r_2 axis at $r_2 = 1$. From this we conclude that within the parameter space for α, r_1, r_2 that gives $p_T^{SC} > p_s^U$, any gain can in principle be obtained. Again, if detectors have efficiency η , then the same conditions apply, with α^2 replaced by $\eta\alpha^2$. Inefficient detectors thus mean that the state comparison amplifier can retain a true success probability which is higher than the unambiguous success probability for somewhat higher amplitude α .

B. Numerical results

After obtaining these bounds regarding success probabilities, it remains to compare the average fidelity of the state comparison amplifier to the average fidelity of the unambiguous measurement, which simply is its success probability. Comparing only success probabilities does not take into account that for the unambiguous measurement, we have perfect fidelity and confidence in the result, while for the state comparison amplifier, we do not. Using the average fidelity as a figure of merit still gives state comparison an advantage in that instances when the guess was incorrect will contribute to the average fidelity. For this reason, we also calculate the confidence in the result, that is, the conditional probability that if the amplifier operates successfully, the guess state was actually right. We also compare with the average fidelity of a random guess. A random guess is wrong half the time but will have the advantage that it always provides a result, which increases the average fidelity. If one wishes,

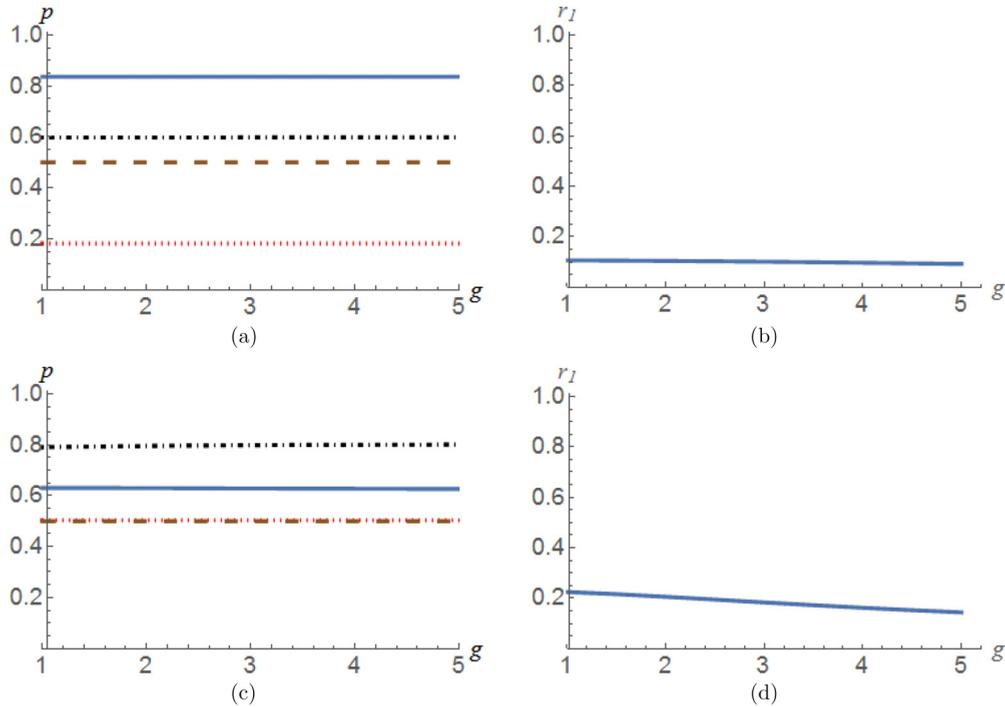


FIG. 2. Plot of success probabilities for $\alpha^2 = 0.1$ and $\alpha^2 = 0.35$. In (a) and (c), we plot the optimal success probability p_s^{SC} for the state comparison amplifier (solid blue line) as a function of amplifier gain. We also plot the success probability p_s^U of the unambiguous measurement (dotted red line; p_s^U is independent of gain and only depends on α^2) and the success probability for a random guess (dashed brown line, always equal to $1/2$). In (a), $\alpha^2 = 0.1$, and in (c), $\alpha^2 = 0.35$. In both cases, the success probability of the state comparison amplifier is higher than that of an unambiguous measurement. However, the confidence in the result is lower for the state comparison amplifier. To illustrate this, we also plot p_T^{SC}/p_s^{SC} , which is the corresponding conditional probability that if the state comparison amplifier is successful, the guess was actually correct (dash-dotted black line). The corresponding conditional probability for the unambiguous measurement is equal to 1, as a successful measurement always gives a correct result. For a random guess the confidence is $1/2$. The confidence in the state comparison result is about 0.6 for $\alpha^2 = 0.1$ and about 0.8 for $\alpha^2 = 0.35$. Plots (b) and (d) show the reflection coefficient r_I corresponding to the optimal state comparison success probabilities p_s^{SC} given in (a) and (c).

one can allow a random guess to be made if the state comparison amplifier and the unambiguous measurement are unsuccessful. We have, however, opted not to do so here, since this would lower the confidence in the result, and also, the output of a probabilistic amplifier would typically be used in a heralded way, conditioned on the device having succeeded.

For varying α^2 and gain, we numerically optimize both success probability and fidelity of the state comparison amplifier given in Eqs. (2) and (6). The optimal success probability does not occur for exactly the same amplifier parameters as the optimal average fidelity. The optimization is done using MATHEMATICA, and either r_1, t_1, r_2 , or t_2 can be taken as the free parameter over which to optimize for fixed α^2 and gain.

We plot the resulting optimal success probabilities in Fig. 2 and optimal average fidelities in Fig. 3, as a function of gain, for $\alpha^2 = 0.1$ and $\alpha^2 = 0.35$. We also plot the success probability of an unambiguous measurement, which is equal to its average fidelity and only depends on α (the gain is in principle unlimited), and the success probability and fidelity of a random guess. The value $\alpha^2 = 0.1$ is in the regime where we expect the state comparison amplifier to have a higher success probability than the unambiguous measurement, while the value $\alpha^2 = 0.35$ is roughly at the boundary where the

true success probability of the state comparison amplifier can no longer exceed that of an unambiguous measurement. We have investigated more values of α^2 , but results for these two cases suffice for illustrating the behavior in the regime of interest.

For $\alpha^2 = 0.1$, we see that the optimal success probability for state comparison is relatively constant at just over 0.8 for the investigated range of gain. It is indeed much higher than that of the unambiguous measurement at about 0.2, but at the expense of significantly lower confidence in the result (about 0.6). For $\alpha^2 = 0.35$, the optimal success probability of the state comparison amplifier is relatively constant at just over 0.6, compared with an unambiguous success probability of about 0.5. (The state comparison “true success” probability, however, will be slightly lower than the success probability of either a random guess or an unambiguous measurement.) It may seem counterintuitive that the total success probability for the state comparison amplifier should be lower for a higher value of α^2 , but recall that success is conditioned on detector $D1$ not firing, and that as a consequence, there is a greater chance of success also of the guess being wrong if α^2 is lower. For $\alpha^2 = 0.35$, the confidence in the result for state comparison is about 0.8.

For $\alpha^2 = 0.1$, the optimal average fidelity of the state comparison amplifier is higher than that of the unambiguous

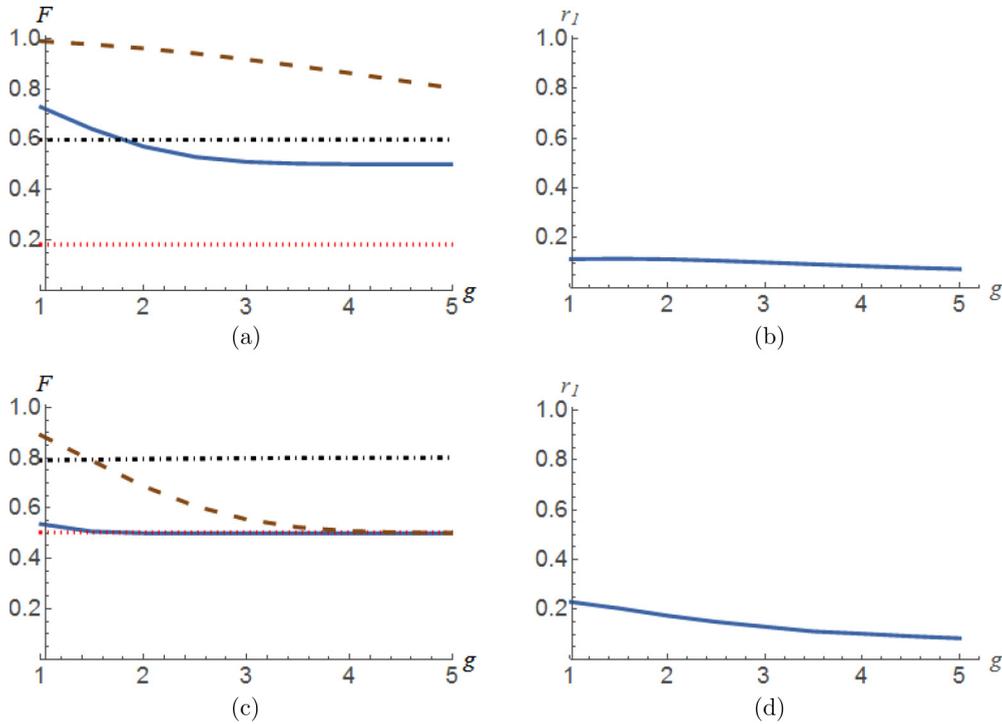


FIG. 3. Plot of average fidelities for $\alpha^2 = 0.1$ and $\alpha^2 = 0.35$. In (a) and (c) we plot the optimal average fidelity F^{SC} for the state comparison amplifier (solid blue line) as a function of amplifier gain. We also plot the fidelity for the unambiguous measurement, which is equal to its success probability p_s^U (dotted red line; p_s^U is independent of gain and only depends on α^2), and the fidelity for a random guess (dashed brown line). In (a), $\alpha^2 = 0.1$, and in (c), $\alpha^2 = 0.35$. While the fidelity of the state comparison amplifier is higher than that of an unambiguous measurement for $\alpha^2 = 0.1$, the random guess has the highest fidelity. For $\alpha^2 = 0.35$, state comparison and an unambiguous measurement both have an average fidelity of about 0.5, while the fidelity for a random guess is higher for low gain and approaches 1/2 for large gain. However, in both (a) and (c), the confidence in the result is lower for the state comparison amplifier. To illustrate this, we also plot p_r^{SC}/p_s^{SC} , the corresponding conditional probability that if the state comparison amplifier is successful, the guess was actually correct (dash-dotted black line). The confidence in the state comparison result is about 0.6 for $\alpha^2 = 0.1$ and about 0.8 for $\alpha^2 = 0.35$. The corresponding conditional probability for the unambiguous measurement is equal to 1, as a successful measurement always gives a correct result. For a random guess the confidence is 1/2. Plots (b) and (d) show the reflection coefficient r_1 corresponding to the optimal state comparison success probability p_s^{SC} given in (a) and (c).

measurement, but a random guess will have an even higher fidelity, also for moderately high gain. The confidence in the result is perfect for an unambiguous measurement and equal to about 0.6 for the state comparison amplifier. This is only somewhat higher than 1/2, which is the confidence for a random guess. As for average fidelities for $\alpha^2 = 0.35$, these are close to 1/2, both for state comparison and an unambiguous measurement over the entire range of gain investigated. Fidelity is higher for a random guess, except for larger gain, when the fidelity of a random guess must approach 1/2. The confidence in the state comparison result is about 0.8.

To summarize, for low amplitudes α^2 , the state comparison amplifier can have a success probability and average fidelity which is higher than that of an unambiguous measurement. However, its fidelity does not beat that of a random guess, unless of course one allows a random guess to be made in the case where the amplifier is not successful. The confidence in the result is perfect for an unambiguous measurement, and 1/2 for a random guess. The confidence for the state comparison amplifier lies somewhere in between, and it can be seen as interpolating between an unambiguous measurement and a random guess in that one trades confidence in the result for average fidelity.

V. AMPLIFIERS IN LOSSY COMMUNICATION CHANNELS

We now consider a situation as in Fig. 4, where a coherent state $|\alpha\rangle$ or $|\alpha\rangle$ is to be transmitted through a lossy quantum channel of length L with decay coefficient γ . This channel transforms a coherent state $|\alpha\rangle$ to $|e^{-\gamma L}\alpha\rangle$. Our figure of merit will be the probability to unambiguously distinguish the two original input states from each other at the end of the channel. If no amplification is used, then this success probability is given by

$$p_{s,1}^U = 1 - \exp(-2e^{-2\gamma L}\alpha^2). \quad (17)$$

We will find that in some cases this can be improved by a measure-and-resend strategy.

A. Measure-and-resend in a lossy communication channel

Assume that an unambiguous measurement is made halfway, after a distance of $L/2$, as indicated in Fig. 4. (We will shortly show that in the scenario we will be considering, measuring halfway is optimal.) If the measurement is successful, then a new state is prepared with the original amplitude

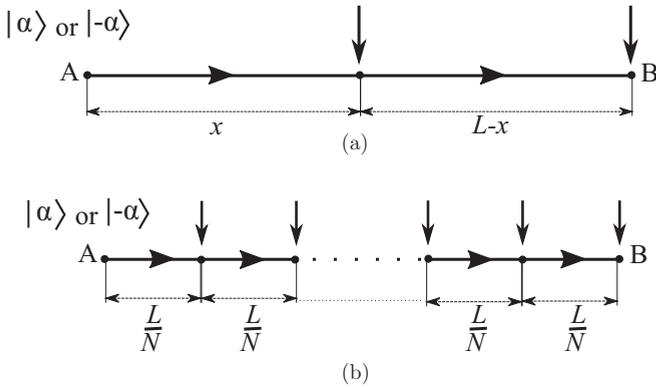


FIG. 4. Intermediate measurements for probabilistic quantum amplification. In (a), one intermediate measurement is made halfway between sender and receiver, and if it is successful, an amplified state can be retransmitted. In (b), a total of N unambiguous measurements are made, including the final measurement.

and resend, and a final unambiguous measurement made at the end. The overall probability for both the intermediate and the final unambiguous measurements to be successful is then given by

$$p_{s,2}^U = [1 - \exp(-2e^{-\gamma L}\alpha^2)]^2. \quad (18)$$

The end receiver also needs to be informed whether the intermediate measurement was successful or not. Otherwise, when no state has been resent, the final measurement result is no longer unambiguous.¹

The amplitude for the retransmitted state can be arbitrarily chosen. Trivially, the higher the gain, the better the overall success probability would be; the limit of infinite gain would correspond to retransmission of classical information. We opt for amplification back to the original amplitude, since whatever reasons determined the original choice of amplitude may still apply for retransmission. In quantum cryptography, for example, the amplitude is limited in order to bound the information an eavesdropper can learn.

An intermediate measurement and retransmission will increase the overall probability for a receiver at the end of the communication channel to distinguish the original input states if $p_{s,1}^U < p_{s,2}^U$, that is, if

$$1 - \exp(-2e^{-2\gamma L}\alpha^2) < [1 - \exp(-2e^{-\gamma L}\alpha^2)]^2. \quad (19)$$

It does not appear straightforward to obtain an explicit solution to this inequality in terms of α and γL . However, as we will show analytically below, if the initial $\alpha^2 > 1/2$, then as γL increases, at some point it becomes advantageous to make a measurement halfway and resend the state with the original amplitude [that is, the right-hand side in Eq. (19) becomes greater than the left-hand side]. If $\alpha^2 \leq 1/2$, then no matter

¹If the end receiver is not informed of whether the intermediate measurement is successful or not, then to keep the result unambiguous, they would have to distinguish between three states, $|\alpha\rangle$, $|- \alpha\rangle$, and $|0\rangle$. Since these states are linearly independent, this is possible in principle; the success probability will, however, be lower, and the optimal measurement more involved.

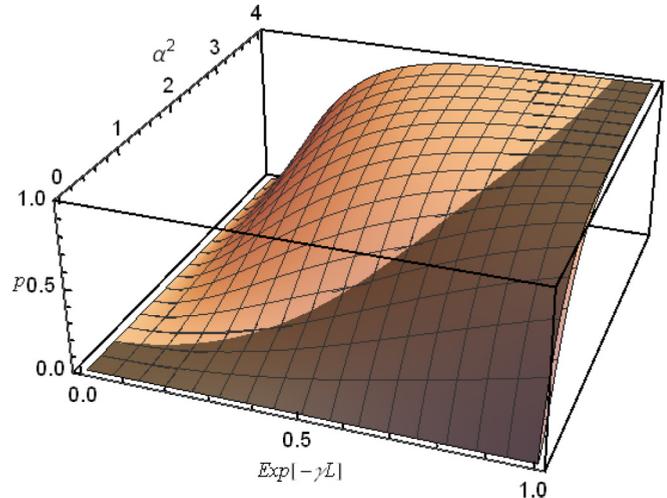


FIG. 5. The success probabilities $p_{s,2}^U$ (lighter surface) and $p_{s,1}^U$ (darker surface). If $\alpha^2 > 1/2$, then when the loss becomes high enough, an intermediate measurement will increase the probability that an end receiver will be able to unambiguously distinguish between the two input states.

how large the loss and transmission distance is, an intermediate measurement never helps (unless, of course, one is allowed to resend with a sufficiently high amplitude). If the detectors have efficiency η , then in all expressions for success probabilities, the effect is to replace α^2 by $\eta\alpha^2$. Thus, in this case, an intermediate imperfect measurement and retransmission can help, compared with just an imperfect measurement at the end, if $\eta\alpha^2 > 1/2$, and γL is high enough.

In Fig. 5, we plot the overall probabilities for an end receiver to distinguish between the original states, with and without an intermediate measurement, as a function of α^2 and $e^{-\gamma L}$. We see that for sufficiently high loss, an intermediate measurement will help. We also see in Fig. 6 that in some regimes, the difference can be appreciable between making only a final measurement and also making an intermediate measurement. As we might expect, in the “classical” regime where α^2 is large and the loss is significant, an intermediate measurement makes a larger difference. The advantage is smaller if the loss becomes too great, illustrating that the signal needs to be reamplified before too much of it has been lost.

B. Many intermediate measurements

Let us now generalize to N measurements, made at distances L/N apart from each other, as shown in Fig. 4(b). We will show that intermediate measurements can help if the initial intensity $\alpha^2 > 1/2$. If a measurement is successful, then the state is retransmitted with the original amplitude, together with the information that all previous measurements were successful. Each of the total N measurements has the same success probability. The overall success probability is therefore

$$p_{s,N}^U = [1 - \exp(-2e^{-2\gamma L/N}\eta\alpha^2)]^N, \quad (20)$$

where, again, η is the efficiency of the detectors (assuming that they all have the same efficiency).

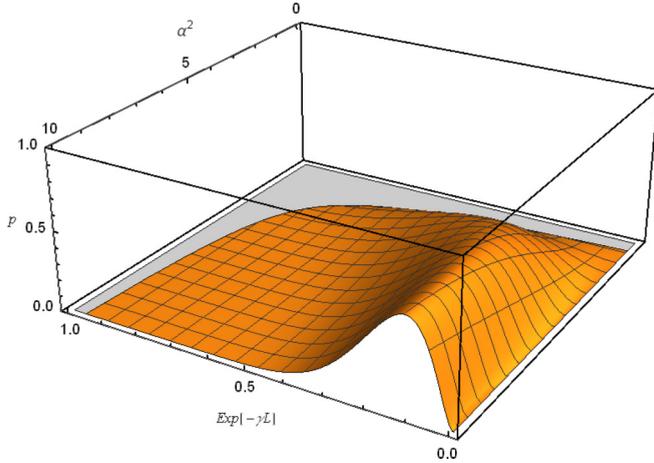


FIG. 6. The difference $p_{s,2}^U - p_{s,1}^U$ between the success probability of an end receiver to distinguish between initial coherent states $|\alpha\rangle$ and $|\alpha\rangle$, if also an intermediate measurement is made ($p_{s,2}^U$), and if only a final measurement is made ($p_{s,1}^U$). In the gray region, it holds that $p_{s,1}^U > p_{s,2}^U$. We see that the difference in success probability can become appreciable, about 0.5. The advantage with a single intermediate measurement is greater for higher α^2 and for high—but not too high—loss. This illustrates the fact that the signal in this regime has to be reamplified before it has decayed too much.

In Fig. 7, we plot the success probabilities $p_{s,N}^U$ for $N \in \{1, 2, 3, 4\}$, as a function of $e^{-2\gamma L}$, for $\eta\alpha^2 \in \{2, 0.5, 0.3\}$. (Plotting as a function of $e^{-2\gamma L}$ rather than $e^{-\gamma L}$ more clearly illustrates the behavior.) We find that for $\eta\alpha^2 > 1/2$, as the total effective loss factor γL increases, the optimal number of intermediate measurements increases. For $\eta\alpha^2 \leq 1/2$, intermediate measurements never improve the situation, irrespective of loss. To confirm this analytically, note first that as $\gamma L \rightarrow \infty$, meaning that $e^{-\gamma L}$ (and $e^{-2\gamma L}$) approaches zero, all success probabilities $p_{s,N}^U$ approach zero, irrespective of $\eta\alpha^2$; if all the signal is lost, one can no longer distinguish between the different input states. To see what happens when $e^{-\gamma L}$ increases, starting from zero, note that the derivative of $p_{s,N}^U$ with respect to $y = e^{-\gamma L}$ is

$$\frac{dp_{s,N}^U}{dy} = 2y^{\frac{1}{N}-1} \eta\alpha^2 [1 - \exp(-2y^{\frac{1}{N}} \eta\alpha^2)]^{N-1} \times \exp(-2y^{\frac{1}{N}} \eta\alpha^2). \quad (21)$$

This expression approaches $(2\eta\alpha^2)^N$ as $e^{-\gamma L}$ approaches zero, as can be seen by making a Taylor expansion for small $y = e^{-\gamma L}$. Hence, if $\eta\alpha^2 > 1/2$, then the higher N is, the steeper the rise of $p_{s,N}^U$ is when $e^{-\gamma L}$ increases starting from zero, as can be seen in Fig. 7(a). However, eventually, when $\gamma L \rightarrow 0$, meaning that $e^{-\gamma L} \rightarrow 1$, the success probability $p_{s,N}^U$ approaches $[1 - \exp(-2\eta\alpha^2)]^N$. This means that $p_{s,N}^U$ for $\gamma L = 0$ decreases with increasing N , for any nonzero $\eta\alpha^2$. (If $\eta\alpha^2 = 0$, then all success probabilities are obviously zero.) That is, for low enough noise, intermediate measurements do not help.

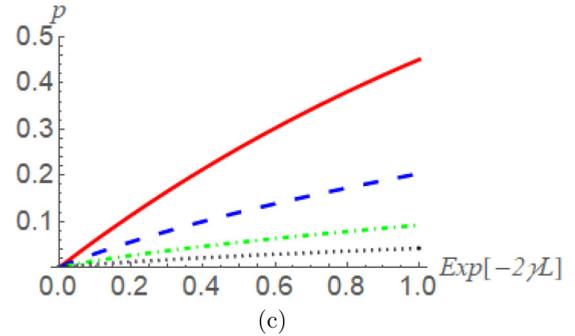
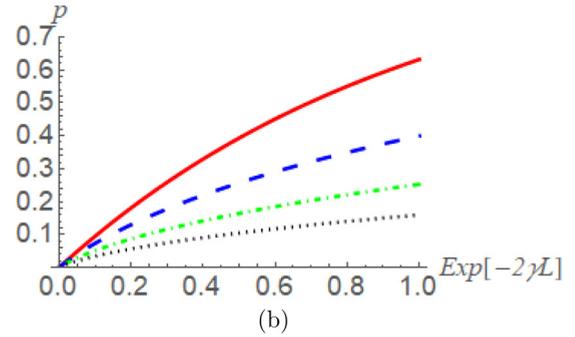
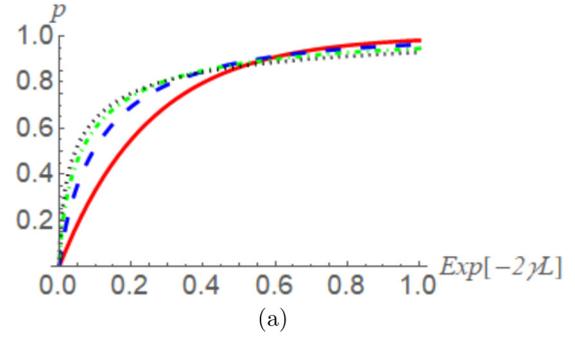


FIG. 7. Overall success probabilities $p_{s,N}^U$, for N equally spaced unambiguous measurements in a lossy channel, as a function of the loss factor $e^{-2\gamma L}$, for $N = 1$ (solid red line), $N = 2$ (dashed blue line), $N = 3$ (dash-dotted green line), and $N = 4$ (dotted gray line). In (a), $\eta\alpha^2 = 2$, and for increasing loss (closer to the origin), the optimal number N of intermediate measurements increases. This illustrates the fact that for any $\eta\alpha^2 > 1/2$, intermediate measurements will improve the situation. (b) For $\eta\alpha^2 = 0.5$ and (c) for $\eta\alpha^2 = 0.3$, intermediate measurements will never help. In all three figures, when the channel becomes lossless, that is, $\exp(-2\gamma L) \rightarrow 1$, the probabilities $p_{s,N}^U \rightarrow [1 - \exp(-2\eta\alpha^2)]^N$. This means that $p_{s,N}^U$ decreases with increasing N for $\gamma L = 0$, which can also be seen in the figures.

This taken together, we conclude that if $\eta\alpha^2 > 1/2$, then as γL increases, so does the optimal number of intermediate measurements. First, one intermediate measurement is better than none. Then two measurements, three, and so on, become optimal, as shown in Fig. 7. If $\eta\alpha^2 \leq 1/2$, then the higher N is, $p_{s,N}^U$ will rise less steeply when $e^{-\gamma L}$ increases starting from zero. Higher numbers of intermediate measurements will then never improve the situation, no matter how large γL becomes, as confirmed by Fig. 7. In Fig. 8, we plot $p_{s,N}^U$ as a function of both α^2 and $e^{-\gamma L}$ for $N = 1$ to $N = 4$, to further illustrate and confirm these results.

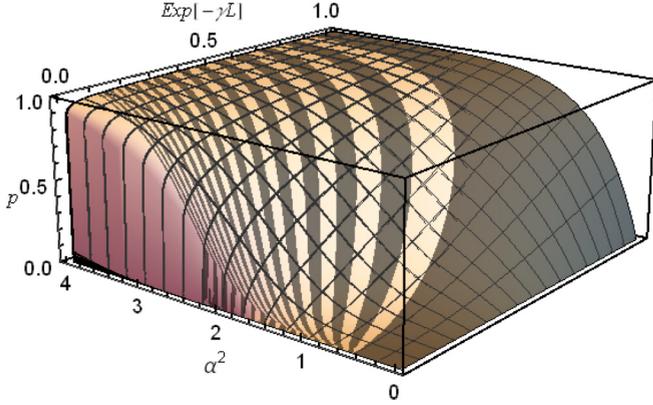


FIG. 8. Overall success probabilities $p_{s,N}^U$, for N equally spaced unambiguous measurements in a lossy channel, as a function of α^2 (with $\eta = 1$) and $e^{\gamma L}$, for increasing numbers of intermediate measurements. The regions where only a final measurement, one intermediate measurement, two, three, etc. are optimal are shown using dark and light stripes, starting with the largest dark region on the right side of the figure, where only a final measurement is optimal. For practical reasons, regions are plotted only until $N = 32$.

C. Optimal number of measurements

We can further show that the optimal number of measurements will increase approximately linearly with γL if $\eta\alpha^2 > 1/2$. To confirm this, consider N to be a continuous variable, and consider $p_{s,N}^U$ as a function of N . To find the optimal N giving the maximum probability $p_{s,N}^U$, we look for solutions to $dp_{s,N}^U/dN = 0$. We have that

$$\frac{dp_{s,N}^U}{dN} = p_{s,N} \left\{ \ln[1 - \exp(-2z\eta\alpha^2)] - \frac{2z\eta\alpha^2 \ln z}{\exp(2z\eta\alpha^2) - 1} \right\}, \quad (22)$$

where $z = e^{-2\gamma L/N}$. The optimal (continuous) value of N is therefore determined by the solutions to the equation

$$\ln[1 - \exp(-2z\eta\alpha^2)] = \frac{2z\eta\alpha^2 \ln z}{\exp(2z\eta\alpha^2) - 1}, \quad (23)$$

for given $\eta\alpha^2$ and γL . Even without obtaining a closed-form solution for the optimal N , we observe that γ , L , and N occur only in the combination $\gamma L/N$. This means that if there is a solution z_0 to Eq. (23), then the optimal (continuous) value of N must increase linearly with γL . Restricting N to discrete values, the optimal N will be the integer value just above or below the optimal continuous N . All in all, this means that the optimal (discrete) number of measurements made along the communication channel increases approximately linearly with γL , for $\eta\alpha^2 > 1/2$, which is when intermediate measurements help at all.

We can also obtain the approximate scaling, as a function of γL , of the overall success probability for the optimal N , for large γL . We can write the success probability $p_{s,N}^U$ in Eq. (20) as

$$p_{s,N}^U = [1 - \exp(-2e^{-2\gamma L/N} \eta\alpha^2)]^N = e^{-A\gamma L}, \quad (24)$$

where

$$A = -\frac{N}{\gamma L} \ln[1 - \exp(-2e^{-2\gamma L/N} \eta\alpha^2)]. \quad (25)$$

For the optimal choice of the (discrete) N , $\gamma L/N$ is approximately constant for large N and γL . Therefore, A is determined by η and α^2 but approximately does not change if, for increasing γL , we also increase the number of intermediate measurements to keep N optimal. Equation (24) therefore shows us how, for a given $\eta\alpha^2$, the success probability for the optimal choice of N scales as a function of increasing γL . The optimal value of $\gamma L/N$ for given $\eta\alpha^2$, and hence the value of A , is given by Eq. (23).

When there are no intermediate measurements, only a final measurement, then the success probability $p_{s,1}^U$ behaves approximately as $2\eta\alpha^2 e^{-2\gamma L}$ for large γL . The scaling of $p_{s,N}^U$ when choosing the optimal value of N , for increasing and large γL , is also approximately exponential but with a modified “decay coefficient” which depends on $\eta\alpha^2$. It can be shown through Taylor expansions that for $\eta\alpha^2 \rightarrow 1/2^+$, the scaling of the optimal $p_{s,N}^U$ approaches $e^{-2\gamma L}$. For other $\eta\alpha^2$, the modified decay coefficient is smaller, meaning that $p_{s,N}^U$ does not decay as fast as a function of γL .

D. Optimal positions of intermediate measurements

Finally, we will show that if intermediate measurements are made, with retransmission of the state with the original amplitude, then it is optimal to make the measurements equidistant from each other. Suppose first that only one intermediate measurement is made, at a distance x from the sender. The overall success probability is then

$$p_{s,2}^U(x) = \{1 - \exp[-2e^{-2\gamma x} \eta\alpha^2]\} \times \{1 - \exp[-2e^{-2\gamma(L-x)} \eta\alpha^2]\}, \quad (26)$$

which is maximized when $x = L/2$, since $1 - \exp(-2e^{-2\gamma x} \eta\alpha^2)$ is a concave function of x , and for a concave function $f(x)$ it holds that $f(x)f(L-x)$ is maximized for $x = L/2$. It follows that for any fixed number of intermediate measurements, these should always be equally spaced in order to optimize the success probability for the end receiver to distinguish the original input states.

E. State comparison versus measure-and-resend in a lossy communication channel

We will now investigate whether a state comparison amplifier, positioned halfway in a lossy communication channel, can improve the probability for an end receiver to unambiguously distinguish between two possible input states $|\pm\alpha\rangle$. In this section, we will take $\eta = 1$ for the detector efficiencies. The improvement should be with respect to “doing nothing” in the channel, or with respect to one or more intermediate unambiguous measurements, whichever is better. The gain will be chosen so that if the amplification is successful (and the guess state is right), then the state will be amplified back to its original amplitude, that is, $g = e^{\gamma L/2}$. The end receiver also needs to know whether the state comparison amplifier was successful or not. If they do not know whether detectors $D1$ and $D2$ fired or not, then the effect of using the amplifier is to divert

some of the incoming amplitude to the detectors, where it is “lost.” This inevitably decreases the ability of an end receiver to tell the input states apart. Even if the guess state is known to the end receiver, using the amplifier evidently cannot increase their probability to distinguish the two input states unless the end receiver also knows whether the amplification succeeded or not.

We will therefore consider the case where the end receiver knows whether or not the state comparison amplifier was successful. They will attempt to make a final measurement only if the amplification was successful. There are still two possibilities: either the end receiver does not know what the guess state was or they do know this. If they do not know what the guess state was, then the end receiver has to distinguish between two equiprobable mixed states, corresponding to whether the input state was $|\alpha\rangle$ or $|\alpha\rangle$. If the guess state is known, then the end receiver should distinguish between two pure coherent states with unequal prior probabilities. In order to give a maximal benefit to the state comparison amplifier, we will here consider the latter case. In a cryptographic scenario, the sequence of guess states could be predetermined, either in secret or publicly known. Note, however, that if the sequence of guess states is secret, known only to sender and receiver, then this would already amount to a shared secret key. This means that if the state comparison amplifier is used for quantum cryptography, either the guess state should be publicly known to everybody, including the receiver, or it should be unknown to everybody, including the receiver.

In the case we are considering, therefore, the end receiver knows what the guess state was and that the state comparison amplification has been successful. They want to learn whether the guess matched the initial state or not. Without loss of generality, we can assume that the guess state was $|\alpha\rangle$. (If the guess state is $|\alpha\rangle$, then the success probability for the final measurement will be the same.) If the initial state was $|\alpha\rangle$, that is, the guess is correct, and the amplification succeeds, then the state received at the end is $|\psi_T\rangle = |e^{-\gamma L} g \alpha\rangle = |e^{-\gamma L/2} \alpha\rangle$. This occurs with the overall probability of p_T^{SC} given in Eq. (4) but with α replaced with $e^{-\gamma L/2} \alpha$, which is now the input amplitude for the state comparison amplifier positioned halfway. If the initial state was $|\alpha\rangle$, that is, the guess was incorrect, then the state received at the end is $|\psi_F\rangle = |e^{-\gamma L} g \alpha(t_1^2 - r_1^2)\rangle = |e^{-\gamma L/2} \alpha(t_1^2 - r_1^2)\rangle$, which occurs with the overall probability of p_F^{SC} given in Eq. (5), but again with α replaced with $e^{-\gamma L/2} \alpha$.

Two pure quantum states $|\psi_1\rangle, |\psi_2\rangle$ with unequal prior probabilities $p_1 = p$ and $p_2 = 1 - p$, where $p \geq 1 - p$, can be unambiguously distinguished from each other with the minimum failure probability [22–24]:

$$p_f = \begin{cases} 2\sqrt{p(1-p)}|\langle\psi_1|\psi_2\rangle| & \text{if } \frac{1-p}{p} \geq |\langle\psi_1|\psi_2\rangle|^2, \\ 1 - p(1 - |\langle\psi_1|\psi_2\rangle|^2) & \text{if } \frac{1-p}{p} \leq |\langle\psi_1|\psi_2\rangle|^2. \end{cases} \quad (27)$$

In the first case, the measurement has three outcomes corresponding to “ $|\psi_1\rangle$,” “ $|\psi_2\rangle$,” and “fail.” In the second case, the measurement has two outcomes, “ $|\psi_1\rangle$ ” and “fail,” and is a projection in the basis $|\psi_2\rangle, |\psi_2^\perp\rangle$, which never succeeds if the state is $|\psi_2\rangle$ but succeeds with probability $1 - |\langle\psi_2|\psi_1\rangle|^2$ if the state is $|\psi_1\rangle$.

In our case, it always holds that $p_T^{SC} > p_F^{SC}$. Depending on other parameters, such as α and γL , one or the other type of measurement may be optimal. The overlap between the two possible states is given by

$$\begin{aligned} |\langle\psi_T|\psi_F\rangle| &= |\langle e^{-\gamma L} g \alpha | e^{-\gamma L} g \alpha (t_1^2 - r_1^2) \rangle| \\ &= \exp(-2t_2^2 r_1^2 e^{-2\gamma L} \alpha^2) = \exp(-2g^2 r_1^4 e^{-2\gamma L} \alpha^2) \\ &= \exp(-2r_1^4 e^{-\gamma L} \alpha^2), \end{aligned} \quad (28)$$

where in the last line we set $g = e^{\gamma L/2}$. For fixed α and γL , the two states become less distinguishable when r_1 decreases. The gain is given by $g = t_2/r_1$, indicating that for a desired gain, we should pick the largest possible t_2 and r_1 giving that gain in order to render the output states maximally distinguishable (at least if we for a moment disregard the unequal prior probabilities; these will also affect distinguishability). However, picking t_2 closer to 1 will decrease the probability that the subtraction detector D_2 fires, thus decreasing the overall probability of success for the amplifier itself. The optimum operating parameters for the amplifier are nontrivial to find.

The overall success probabilities for both the state comparison amplification and the final measurement to succeed read, for the three-outcome type of final measurement,

$$p_{s,\text{final}}^{SC} = p_s^{SC} - 2\sqrt{p_T^{SC} p_F^{SC}} |\langle\psi_T|\psi_F\rangle|, \quad (29)$$

which is optimal if $p_F^{SC}/p_T^{SC} \geq |\langle\psi_T|\psi_F\rangle|^2$. The probabilities p_s^{SC} , p_T^{SC} , and p_F^{SC} are given in Eqs. (2), (4), and (5), respectively. For the two-outcome type of final measurement, the overall success probability of amplification and final measurement is

$$p_{s,\text{final}}^{SC} = p_s^{SC} - p_F^{SC} - p_T^{SC} |\langle\psi_T|\psi_F\rangle|^2, \quad (30)$$

which is optimal if $p_F^{SC}/p_T^{SC} \leq |\langle\psi_T|\psi_F\rangle|^2$. Which of these is better, and what the largest possible success probability is will depend on α , γL , and on the beam-splitter coefficients in the state comparison amplifier.

For given α and γL , if we are fixing the gain to be $g = t_2/r_1 = e^{\gamma L/2}$, then there is one remaining parameter to optimize over in the state comparison amplifier. For different fixed values of α and γL (thus also fixing g), we numerically perform this optimization using MATHEMATICA to find the optimal overall success probability for both amplification and final measurement to succeed. The results for $\alpha^2 = 0.5, 0.35$, and 0.1 are plotted in Fig. 9. In this figure, we also plot the success probability $p_{s,1}^U$ for a final unambiguous measurement only, and $p_{s,2}^U$ for one intermediate unambiguous measurement and a final measurement. The numerical results show that a state comparison amplifier unfortunately does not improve the probability of an end receiver to distinguish between the two input coherent states, as compared with $p_{s,1}^U$ for a final unambiguous measurement only. We have also numerically investigated other values of α^2 , larger and smaller, and have been unable to find any case where the state comparison amplifier would increase the overall success probability. For $\alpha^2 = 0.1$, using the state comparison amplifier at least gives a higher success probability than one intermediate measurement. This is consistent with the analytical and numerical results in Sec. IV, which said that for low α^2 , the state comparison

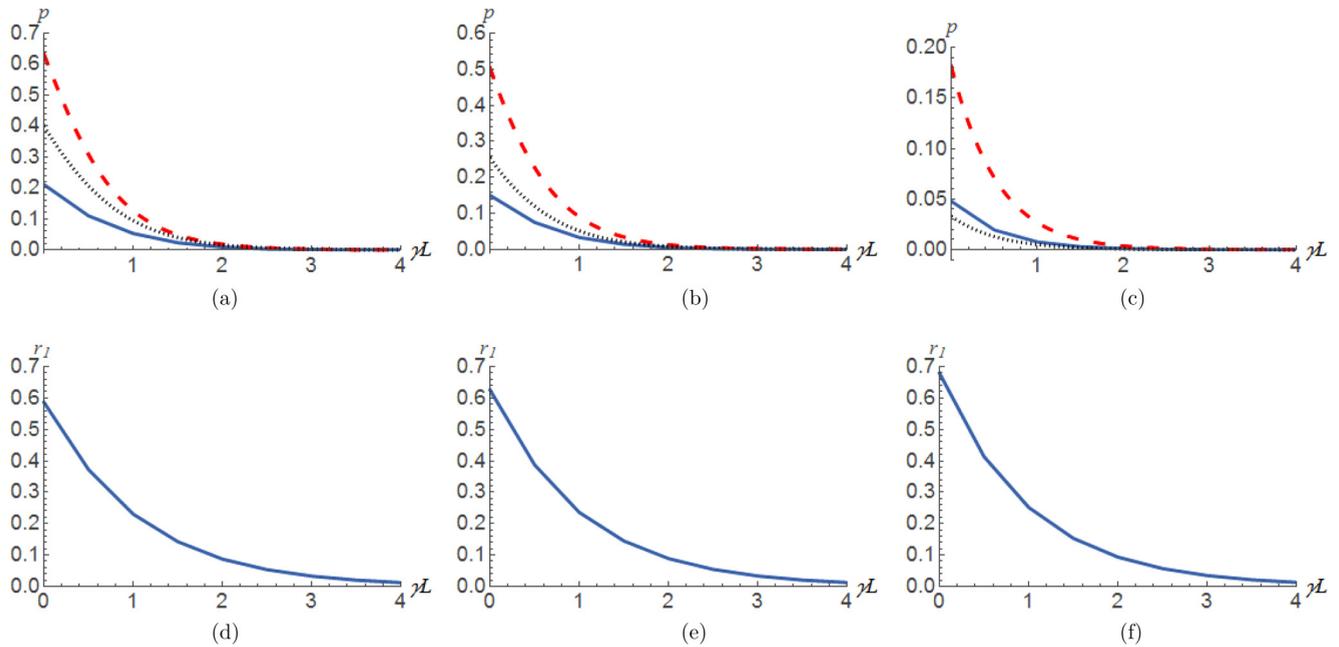


FIG. 9. Success probabilities for a receiver at the end of a lossy channel to distinguish between the initial states $|\pm\alpha\rangle$, for (a) $\alpha^2 = 0.5$, (b) $\alpha^2 = 0.35$, and (c) $\alpha^2 = 0.1$. The solid blue lines in (a), (b), and (c) show the success probability for the end receiver if an optimized state comparison amplifier is situated halfway in the lossy channel. When performing the numerical optimization over r_1 , γL is increased in steps of 0.5. The dashed red lines show the success probability if only a final unambiguous measurement is made, when otherwise only the lossy channel is acting on the input state. The dotted gray lines show the success probability if one intermediate unambiguous measurement is made in addition to the final measurement. The corresponding optimal values for the beam-splitter reflection coefficient r_1 for the state comparison amplifier as a function of γL are given in (d), (e), and (f). The state comparison amplifier does not improve performance for any investigated combinations of α and loss γL . Most of the time, a single final unambiguous measurement is optimal; as we have shown, unless $\alpha^2 > 1/2$, an intermediate unambiguous measurement will never help.

amplifier can have higher success probability and fidelity than an unambiguous measurement.

The fact that state comparison does not seem to improve performance, compared with no action in the lossy channel, is also consistent with the results in Sec. IV. The bounds we obtained said that for the state comparison amplifier to succeed more often than an unambiguous measurement, in the large-gain limit, it had to hold that $\alpha^2 < \ln(\sqrt{2} - 1) \approx 0.44$, and for the true success probability to be larger than the unambiguous success probability, for any gain, it had to hold that $\alpha^2 < (\ln 2)/2 \approx 0.35$. On the other hand, we saw in Sec. V that an intermediate measurement in a lossy channel can only be beneficial if $\alpha^2 > 1/2$. These facts, taken together, make it seem plausible that a state comparison amplifier in a lossy channel is unlikely to improve the situation in any parameter regime, and our numerical investigations confirm this intuition.

VI. CONCLUSIONS

We have learned that intermediate unambiguous measurements in a lossy communication channel, followed by retransmission of the state with the original amplitude, can improve the probability for an end receiver to unambiguously distinguish between two coherent states, but only if $\eta\alpha^2 > 1/2$, where α^2 is the original amplitude and η the efficiency of all detectors. The loss γL also has to be sufficiently high for intermediate measurements to help. We again want to

note that since the information on whether the intermediate measurements succeeded or not has to be transmitted along with the resent state, the measure-resend procedure does not increase the capacity of the channel to carry classical information in the scenario we are considering.

In quantum key distribution, one generally uses coherent states with intensities that are below $1/2$, and there are restrictions on how large the loss can be, which is typically in the range of 3 dB [28,29]. Koashi found for the B92 protocol that for an amplitude of $\alpha^2 = 1/2$, positive key rates require a near-perfect realization [30]. Our results thus confirm the intuition that measure-resend strategies are unlikely to be useful for quantum cryptography, in addition to the fact that the measurements would have to be performed in secure nodes.

Even though for low amplitudes for the input state the success probability and the average fidelity of the state comparison amplifier can be higher than those of an unambiguous measurement, we have been unable to find a parameter regime where the state comparison amplifier would improve the situation if used in a lossy communication channel. This does not completely rule out the possibility of state comparison amplifiers being useful in quantum communication networks, but it does make it look much less likely.

However, the state comparison amplifier we have investigated can actually be improved. If detector D_1 fires, in which case that the amplifier is unsuccessful, then we actually know that the guess state was incorrect. Hence we know with certainty what the input state was, but this knowledge is not

used. A modified version of the state comparison amplifier [31] uses feed-forward operations to retransmit an amplified state also in this case. The device is no longer as simple to realize, but its performance is better. It would be of interest to benchmark also this improved state comparison amplifier. Other possible questions would be to investigate when varying where in the lossy channel a state comparison amplifier is situated. Also, we have fixed the gain to give amplification back to the original amplitude, but in principle a lower gain should also be allowed. One might also investigate the effect

of more than one intermediate state comparison amplifier in a lossy channel.

ACKNOWLEDGMENTS

The authors acknowledge helpful discussions with J. Jeffers and L. Mazzarella. I.V.P. and E.A. acknowledge financial support by the EPSRC Quantum Technology Hub for Quantum Communications through Grant No. EP/M013472/1.

-
- [1] D. T. Pegg, L. S. Phillips, and S. M. Barnett, Optical State Truncation by Projection Synthesis, *Phys. Rev. Lett.* **81**, 1604 (1998).
- [2] T. C. Ralph and A. P. Lund, in *Proceedings of the 9th International Conference on Quantum Communication, Measurement and Computing*, edited by A. Lvovsky (AIP, Melville, NY, 2009), p. 155.
- [3] J. Fiurášek, Engineering quantum operations on traveling light beams by multiple photon addition and subtraction, *Phys. Rev. A* **80**, 053822 (2009).
- [4] P. Marek and R. Filip, Coherent-state phase concentration by quantum probabilistic amplification, *Phys. Rev. A* **81**, 022302 (2010).
- [5] J. Jeffers, Optical amplifier-powered quantum optical amplification, *Phys. Rev. A* **83**, 053818 (2011).
- [6] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Heralded noiseless linear amplification and distillation of entanglement, *Nat. Photon.* **4**, 316 (2010).
- [7] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, Implementation of a Nondeterministic Optical Noiseless Amplifier, *Phys. Rev. Lett.* **104**, 123603 (2010).
- [8] A. Zavatta, J. Fiurášek, and M. Bellini, A high-fidelity noiseless amplifier for quantum light states, *Nat. Photon.* **5**, 52 (2011).
- [9] M. A. Usuga, C. R. Müller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, Noise-powered probabilistic concentration of phase information, *Nat. Phys.* **6**, 767 (2010).
- [10] N. Gisin, S. Pironio, and N. Sangouard, Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier, *Phys. Rev. Lett.* **105**, 070501 (2010).
- [11] D. Pitkanen, X. Ma, R. Wickert, P. van Loock, and N. Lütkenhaus, Efficient heralding of photonic qubits with applications to device-independent quantum key distribution, *Phys. Rev. A* **84**, 022325 (2011).
- [12] N. Bruno, V. Pini, A. Martin, and R. T. Thew, A complete characterization of the heralded noiseless amplification of photons, *New J. Phys.* **15**, 093002 (2013).
- [13] D. Menzies and S. Croke, Noiseless linear amplification via weak measurements, [arXiv:0903.4181](https://arxiv.org/abs/0903.4181).
- [14] V. Dunjko and E. Andersson, Truly noiseless probabilistic amplification, *Phys. Rev. A* **86**, 042322 (2012).
- [15] J. Jeffers, Nondeterministic amplification for two-photon superpositions, *Phys. Rev. A* **82**, 063828 (2010).
- [16] S. M. Barnett and D. T. Pegg, Optical state truncation, *Phys. Rev. A* **60**, 4965 (1999).
- [17] M. Koniarczyk, Z. Kurucz, A. Gábris, and J. Janszky, General optical state truncation and its teleportation, *Phys. Rev. A* **62**, 013802 (2000).
- [18] S. A. Babichev, J. Ries, and A. I. Lvovsky, Quantum scissors: Teleportation of single-mode optical states by means of a nonlocal single photon, *Europhys. Lett.* **64**, 1 (2003).
- [19] E. Eleftheriadou, S. M. Barnett, and J. Jeffers, Quantum Optical State Comparison Amplifier, *Phys. Rev. Lett.* **111**, 213601 (2013).
- [20] R. J. Donaldson, R. J. Collins, E. Eleftheriadou, S. M. Barnett, J. Jeffers, and G. S. Buller, Experimental Implementation of a Quantum Optical State Comparison Amplifier, *Phys. Rev. Lett.* **114**, 120505 (2015).
- [21] A. Chefles, Unambiguous discrimination between linearly independent quantum states, *Phys. Lett. A* **239**, 339 (1998).
- [22] I. D. Ivanovic, How to differentiate between non-orthogonal states, *Phys. Lett. A* **123**, 257 (1987).
- [23] D. Dieks, Overlap and distinguishability of quantum states, *Phys. Lett. A* **126**, 303 (1988).
- [24] A. Peres, How to differentiate between non-orthogonal states, *Phys. Lett. A* **128**, 19 (1988).
- [25] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, *Phys. Rev. A* **51**, 1863 (1995).
- [26] S. J. van Enk, Unambiguous state discrimination of coherent states with linear optics: Application to quantum cryptography, *Phys. Rev. A* **66**, 042313 (2002).
- [27] S. Croke, E. Andersson, S. M. Barnett, C. Gilson, and J. Jeffers, Maximum Confidence Quantum Measurements, *Phys. Rev. Lett.* **96**, 070401 (2006).
- [28] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Continuous Variable Quantum Cryptography Beating the 3 dB Loss Limit, *Phys. Rev. Lett.* **89**, 167901 (2002).
- [29] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using Gaussian-modulated coherent states, *Nature (London)* **421**, 6920 (2002).
- [30] M. Koashi, Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse, *Phys. Rev. Lett.* **93**, 120501 (2004).
- [31] J. Jeffers and L. Mazzarella (private communication).