

PROCEEDINGS OF SPIE

[SPIDigitalLibrary.org/conference-proceedings-of-spie](https://spiedigitallibrary.org/conference-proceedings-of-spie)

Quantum state comparison amplifier with feedforward state correction

L. Mazzearella, R. J. Donaldson, R. J. Collins, U. Zanforlin, G. Tatsu, et al.

L. Mazzearella, R. J. Donaldson, R. J. Collins, U. Zanforlin, G. Tatsu, G. S. Buller, J. Jeffers, "Quantum state comparison amplifier with feedforward state correction," Proc. SPIE 10674, Quantum Technologies 2018, 106741D (21 May 2018); doi: 10.1117/12.2307818

SPIE.

Event: SPIE Photonics Europe, 2018, Strasbourg, France

Quantum State Comparison Amplifier with Feedforward State Correction

L. Mazzarella^a, R. J. Donaldson^b, R. J. Collins^b, U. Zanforlin^b, G. Tatsu^a, G. S. Buller^b, and J. Jeffers.^a

^aDepartment of Physics, University of Strathclyde, John Anderson Building, 107 Rottenrow, Glasgow G4 0NG, U.K.

^bInstitute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, David Brewster Building, Heriot-Watt University, Edinburgh EH14 4AS, U.K.

ABSTRACT

Quantum mechanics imposes stringent constraints on the amplification of a quantum signal. Deterministic amplification of an unknown quantum state always implies the addition of a minimal amount of noise.¹ Linear and noiseless amplification is allowed in principle provided that it only works probabilistically²³. Here we present a probabilistic amplifier that combines two quantum state comparison amplifiers (SCAMP)⁴ together with a feed-forward state correction strategy. Our system outperforms the unambiguous state discrimination (USD)⁵ measure-and-resend based amplifier in terms of the success probability-fidelity product and requires a no more complex experimental setting.

Keywords: quantum amplifier, state amplification, coherent states, state comparison, probabilistic amplifier, quantum technologies, optical amplifier.

1. INTRODUCTION

The efficient amplification of weak coherent states is important for the implementation of various quantum information processing tasks. For example, weak coherent states are used to encode information in quantum communications protocols such as QKD^{678*} and QDS¹²¹³.

SCAMP is a mature technique that provides approximate probabilistic amplification for a known, symmetric set of coherent states by comparing at a beam splitter the unknown input state with a guess coherent state. The state comparison is shown in figure 1: Alice picks one state from the set at random and provides it to Bob whose task is to amplify it. Bob does so by mixing it with the guess coherent state at the beam splitter in an attempt to achieve destructive interference in one of the arms, monitored by a single-photon avalanche diode (SPAD).¹⁴

From here on, we assume that the state space comprises two states $\{|+\alpha\rangle, |-\alpha\rangle\}$. Higher state spaces are possible but represent an additional degree of complication that we do not need here. Let us also assume that Bob chooses $|\beta_1\rangle = |+\frac{t_1}{r_1}\alpha\rangle$ for his guess. If Alice's input is $|\alpha\rangle$ there will be destructive interference in the detector arm, preventing it from registering an event. In this case we say that Bob's guess was right and the output will be given by the amplified state $|\frac{\alpha}{r_1}\rangle$ (see the appendix A for the detailed calculations of the coherent amplitudes). The device gain is thus given by $g^2 = \frac{1}{r_1^2}$. Note that the gain of the system is linked to the beam splitter parameters. On the other hand, if Bob's guess is incorrect (i.e. $|-\frac{t_1}{r_1}\alpha\rangle$) a non-zero coherent amplitude will be incident on the detector and may or may not cause it to fire. The indication is imperfect because the lack of counts can be due either to the imperfect efficiency of the detector or the non-zero overlap of the coherent state with the vacuum state, so there is still the chance that the guess was wrong. Hence, the detector not firing

Send correspondence to L.M.

L.M.: E-mail: luca.mazzarella@strath.ac.uk.

*originally, such protocols were supposed to use single-photons⁶ but since their on-demand generation is quite challenging⁹¹⁰, practical implementation typically use low intensity laser pulses, modeled as weak coherent states, as the information carriers.¹¹

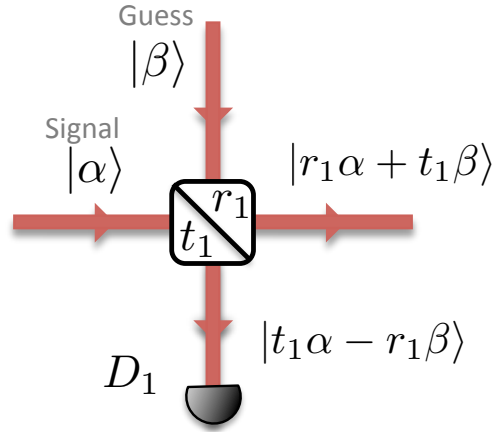


Figure 1. The state comparison amplifier. Bob attempts to achieve destructive interference in the output arm that is fed into the detector D_1 .

represents an *imperfect indication* that Bob's guess was right and that the output contains the amplified version of the input state.

The output state, conditioned on the detector not firing, is thus a mixture of the correct amplified state (when the guess is right) and the wrong amplified state (when the guess is wrong), with the relative weights of the two states in the mixture biased towards the correct state. In summary, Bob declares success and postselects the outcome based on no counts being recorded at the detector. The success probability is given by:

$$P(S) = \sum_{\sigma=\{+\alpha, -\alpha\}} P(\mathbf{x}_1|\beta_1, \sigma)P(\sigma), \quad (1)$$

where $P(\mathbf{x}_1|\beta_1, \sigma)$ is the probability of the detector not firing given a particular input and guess state. As $|+\alpha\rangle$ and $|-\alpha\rangle$ are a priori equally probable we have $P(+\alpha) = P(-\alpha) = \frac{1}{2}$. As mentioned before, SCAMP is an approximate amplifier, i.e. it will sometimes provide the wrong answer. Usually the performance of an amplifier is quantified via the fidelity of its output with the correct amplified state, i.e.:

$$F = \sum_{\sigma=\{+\alpha, -\alpha\}} P(\sigma)\langle g\sigma|\rho_{out}|g\sigma\rangle. \quad (2)$$

This expression is a convex combination of overlaps of the nominal amplified state with the output, conditioned on a particular input and guess. Fidelity can also be seen as the probability of the output passing a measurement test comparing it to the correct amplified state given success. More formally:

$$F = P(T|S) = \frac{P(T, S)}{P(S)}, \quad (3)$$

where $P(S)$ is the device's success probability and $P(T, S)$ is the joint probability of passing the measurement test and success. The numerator can be worked out as follows:

$$P(T, S) = \sum_{\sigma=\{+\alpha, -\alpha\}} P(T|\mathbf{x}_1, \beta_1, \sigma)P(\mathbf{x}_1|\beta_1, \sigma)P(\sigma). \quad (4)$$

The numerator itself is a figure of merit for the device, corresponding to the success probability-fidelity product. It jointly quantifies the output quality and its probability.³

Note also that, if the detector fires, we know that Bob's guess is wrong and in the case of a two state space scenario we know precisely which was the input state. This fact suggests that we could enhance the performance of the comparison system by adding a second comparison stage, provided that we choose the second input state based on the outcome of the first detector. In the next section we will describe a system that implements this feature.

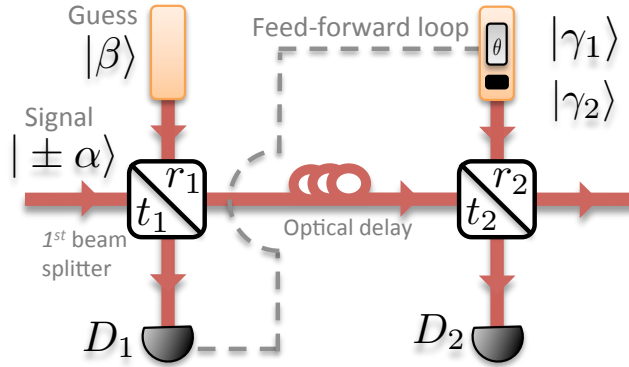


Figure 2. Schematic of the state comparison amplifier with state correction. Bob attempts to achieve destructive interference in both the output arms which are fed into the detectors. This time, if the first detector fires, he can still correct the output by suitably changing the input state of the second comparison stage via the amplitude and phase modulator (in this case the outcome of the second detector is disregarded).

2. SCAMP WITH FEED-FORWARD STATE CORRECTION

Let us now consider a new system comprising of two comparison stages as shown in figure 2. Again, Alice will choose a state uniformly at random while Bob this time has to choose two input states, one for each comparison beam splitter.

The first comparison stage is operated as before. If the first detector does not fire Bob has no reason to believe his initial guess was wrong and will continue the amplification process by mixing the output of the first comparison stage accordingly (i.e., with the state $|\beta_2\rangle = |\frac{t_2}{r_1 r_2}\alpha\rangle$ if he has chosen $|\frac{t_1}{r_1}\alpha\rangle$ at the previous stage) and if also the second detector does not fire he takes this as an imperfect indication that his guess was right and that the output contains the correct amplified state. If Alice's choice was $|+\alpha\rangle$ the output state is given by $|\frac{\alpha}{r_1 r_2}\rangle$, henceforth the gain of the device is given by $g^2 = \frac{1}{r_1^2 r_2^2}$. The device output given both the comparison detectors did not fire is given by:

$$\rho_{\text{out}}|_{\mathbf{x}_1, \mathbf{x}_2} = p \left| \frac{\alpha}{r_1 r_2} \right\rangle \left\langle \frac{\alpha}{r_1 r_2} \right| + (1-p) \left| \frac{2r_1^2 r_2^2 - 1}{r_1 r_2} \alpha \right\rangle \left\langle \frac{2r_1^2 r_2^2 - 1}{r_1 r_2} \alpha \right| \quad \text{with} \quad p = \frac{P(\mathbf{x}_1, \mathbf{x}_2 | +\alpha)}{P(\mathbf{x}_1, \mathbf{x}_2)} P(+\alpha). \quad (5)$$

On the other hand, if the second detector does fire Bob knows for sure that his guess was wrong in first place and simply discards the output. Note that again the probability for both the detectors to not fire is maximised when Bob's guess is right.

Suppose now the first detector does fire, then Bob knows that his guess was wrong but he can still correct the final output if the device allows him to choose the appropriate correcting input state for the second comparison stage. More precisely, suppose Bob's first input was $|\beta_1\rangle = |\frac{t_1}{r_1}\alpha\rangle$, if the first detector fires, Bob can correct the output by inserting in the second beam splitter the state $|\gamma_2\rangle = \left| \frac{1}{t_2} \left(\frac{-1-r_2^2(t_1^2-r_1^2)}{r_1 r_2} \right) \alpha \right\rangle$. In this case there is in principle no need to monitor the second detector counts as Bob knows he is correct.

The success scenarios of the device can be summarised in the following table, where the events corresponding to successful post-selection are highlighted in green:

SCAMP Success Scenario				
D_1	D_2	Bob's input 1 st BS	Bob's input 2 nd BS	Output
✗	✗	$ \frac{t_1}{r_1}\alpha\rangle$	$ \frac{t_2}{r_1 r_2}\alpha\rangle$	$\rho_{\text{out}} _{\mathbf{x}_1, \mathbf{x}_2}$
✗	✓	$ \frac{t_1}{r_1}\alpha\rangle$	$ \frac{t_2}{r_1 r_2}\alpha\rangle$	☠
✓	✗	$ \frac{t_1}{r_1}\alpha\rangle$	$ \frac{1}{t_2} \left(\frac{-1-r_2^2(t_1^2-r_1^2)}{r_1 r_2} \right) \alpha\rangle$	$ \frac{-\alpha}{r_1 r_2}\rangle$
✓	✓	$ \frac{t_1}{r_1}\alpha\rangle$	$ \frac{1}{t_2} \left(\frac{-1-r_2^2(t_1^2-r_1^2)}{r_1 r_2} \right) \alpha\rangle$	$ \frac{-\alpha}{r_1 r_2}\rangle$

Summing up, provided that the correction strategy can be enacted, the successful events are given by the following set of detection outcomes:

$$S = \{ \{D_1 = \mathbf{X}, D_2 = \mathbf{X}\}, D_1 = \checkmark \}. \quad (6)$$

Note that the amplitude of the states $|\beta_2\rangle$ and $|\gamma_2\rangle$ have opposite phases and the second is larger in magnitude[†]. The benefit of the state correction strategy is now apparent, it increases both the success probability and the fidelity, compared to the single comparison stage, by including in the success scenarios an event that corresponds to exact amplification.

3. PERFORMANCE ANALYSIS

Bearing in mind the mechanism by which Bob has to choose the input states at the second stage, we can now compute the success probability for the new device. For sake of simplicity sake we will assume that the two comparison beamsplitters identical, i.e. $r_1 = r_2 = r$, and detection efficiency $\eta_1 = \eta_2 = \eta$:

$$P(S) = P(\mathbf{X}_2, \mathbf{X}_1) + P(\mathbf{X}_2, \checkmark_1) + P(\checkmark_2, \checkmark_1) \quad (7)$$

$$= P(\mathbf{X}_2, \mathbf{X}_1) + P(\checkmark_1) \quad (8)$$

$$= \sum_{\sigma=\{+\alpha, -\alpha\}} (P(\mathbf{X}_2, \mathbf{X}_1|\beta_2, \beta_1, \sigma) + P(\checkmark_1|\beta_1, \sigma)) P(\sigma) \quad (9)$$

$$= \frac{1}{2} \left(1 + e^{-4\eta(1-\frac{1}{g^2})\alpha^2} \right) + \frac{1}{2} \left(1 - e^{-4\eta(1-\frac{1}{g})\alpha^2} \right). \quad (10)$$

Since there is no knowledge about the input state we have that $P(+\alpha) = P(-\alpha) = \frac{1}{2}$. Furthermore we have that $P(\mathbf{X}_2, \mathbf{X}_1|\beta_2, \beta_1, +\alpha) = 1$ and $P(\checkmark_1|\beta_1, +\alpha) = 0$ and the rest of the probabilities are computed in appendix A.

Let us now consider the success probability-fidelity product and as before we assume that Bob's initial guess was $|\beta_1\rangle = |\frac{t_1}{r_1}\alpha\rangle$:

$$P(T, S) = P(T, \mathbf{X}_2, \mathbf{X}_1) + P(T, \checkmark_1) \quad (11)$$

$$= \sum_{\sigma=\{+\alpha, -\alpha\}} (P(T, \mathbf{X}_2, \mathbf{X}_1|\beta_2, \beta_1, \sigma) + P(T, \checkmark_1|\gamma_2, \beta_1, \sigma)) P(\sigma) \quad (12)$$

$$= \sum_{\sigma=\{+\alpha, -\alpha\}} (P(T|\mathbf{X}_2, \mathbf{X}_1, \beta_2, \beta_1, \sigma) + P(T|\checkmark_1, \gamma_2, \beta_1, \sigma) P(\checkmark_1|\beta_1, \sigma)) P(\sigma). \quad (13)$$

The probabilities of passing the measurement test for a given set of input and guess state can be readily computed as:

$$P(T|\mathbf{X}_2, \mathbf{X}_1, \beta_2, \beta_1, +\alpha) = |\langle g\alpha|g\alpha\rangle|^2 = 1, \quad (14)$$

$$P(T|\mathbf{X}_2, \mathbf{X}_1, \beta_2, \beta_1, -\alpha) = |\langle g(1-2/g^2)\alpha| - g\alpha\rangle|^2, \quad (15)$$

$$P(T|\checkmark_1, \gamma_2, \beta_1, +\alpha) = 0, \quad (16)$$

$$P(T|\checkmark_1, \gamma_2, \beta_1, -\alpha) = 1, \quad (17)$$

where $P(T|\checkmark_1, \gamma_2, \beta_1, +\alpha) = 0$ is understood as the detector cannot trigger due to a correct guess. The overlap of two coherent states, say $|\sigma_1\rangle$ and $|\sigma_2\rangle$ is:

$$|\langle\sigma_1|\sigma_2\rangle|^2 = e^{-|\sigma_1-\sigma_2|^2}. \quad (18)$$

The success probability-fidelity product is thus given by:

$$P(T, S) = \frac{1}{2} \left(1 + P(\mathbf{X}_2, \mathbf{X}_1|\beta_2, \beta_1, -\alpha) |\langle g(1-2/g^2)\alpha| - g\alpha\rangle|^2 + P(\checkmark_1|\gamma_2, \beta_1, -\alpha) \right) \quad (19)$$

$$= \frac{1}{2} \left(1 + e^{-4\eta(1-\frac{1}{g^2})|\alpha|^2} e^{-4g^2(1-\frac{1}{g^2})^2|\alpha|^2} + 1 - e^{-4\eta(1-\frac{1}{g})|\alpha|^2} \right). \quad (20)$$

[†]It is easy to see that $\frac{\gamma_2}{\beta_2} = 2t_1^2 \left(\frac{t_2^2-1}{t_2^2} \right) - 1 < 0$ and that $\left| \frac{\gamma_2}{\beta_2} \right| - 1 = 2t_1^2 \left(\frac{1-t_2^2}{t_2^2} \right) > 0$.

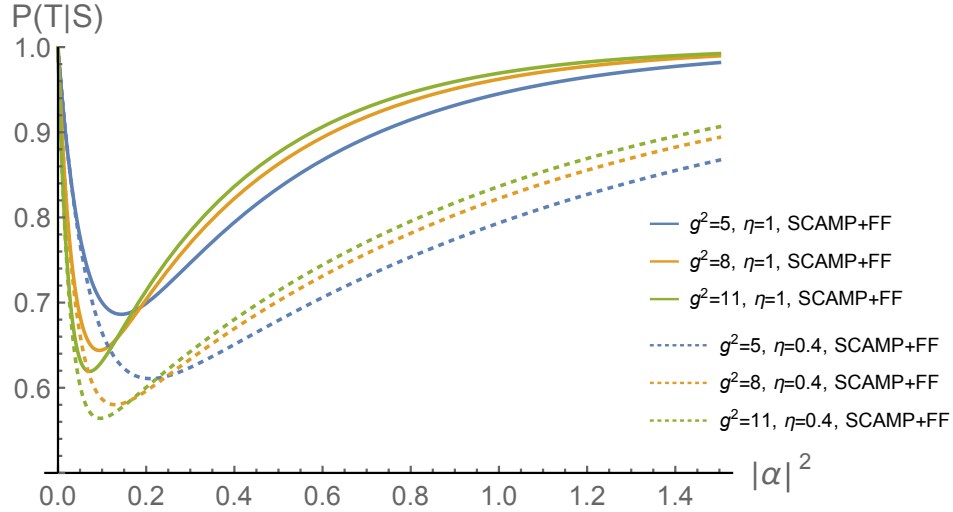


Figure 3. Success probability-fidelity product as a function of the input mean photon number for various values of the gain g^2 for the SCAMP with feedforward state correction. Solid lines (dashed) correspond to a detection efficiency of 1 (0.4).

The success probability-fidelity product is plotted in figure 3. All the curves show a similar pattern: $P(T, S)$ at first decreases until it reaches a minimum, whose position depends on the gain and the detection efficiency, after that it increases until it asymptotically reaches one.

This trend is due to the fact that for low input mean photon number it is very unlikely for the detectors to trigger even when the guess is wrong, this causes $P(T, S)$ to decrease until the probability for the first detector to trigger become significant, thus enacting state correction. As can be appreciated, this turning point is reached for lower mean photon number as the gain increases but it corresponds to a deeper minimum. The effect in the success probability-fidelity product of inefficient detection does not change this behaviour but it pushes the recovery to higher mean photon number as it decreases the probability of registering events at the detectors.

4. COMPARISON WITH UNAMBIGUOUS STATE DISCRIMINATION (USD)

The problem of amplifying an unknown coherent state can be recast as the problem of discriminating between the coherent states in the set and subsequently outputting an amplified version of that state. The optimal probability with which a symmetric set of coherent states, a priori equiprobable and with known mean photon number, can be unambiguously discriminated has been computed in⁵ for an arbitrary state space dimension. For a two state space, the best possible success probability is given by:

$$P_{USD}^{opt} = 1 - e^{-2|\alpha|^2}. \quad (21)$$

Remarkably, the bound can be achieved by using equivalent experimental means to SCAMP, an experimental realisation of it is sketched in figure,⁷ note that feed-forward capability is also needed in this case. The unknown quantum state is mixed at a 50:50 beam splitter with (say) the state $|+\alpha\rangle$, depending on the input state, all the light will go in one of the two output arms while the other will be in the vacuum state. Hence a detector triggering will provide an unambiguous indication of what the input state was, while no detector firing will leave Bob no wiser. The phase modulator imprint the correct phase on the output based on the detection outcomes, the device's gain is given by $g^2 = \frac{t^2}{r^2}$. Taking into account detection inefficiency the previous expression reads:

$$P_{USD} = 1 - e^{-2\eta|\alpha|^2}. \quad (22)$$

We also note that, despite the fact that unambiguous discrimination can be carried out for a bigger state space, there are no linear optical implementations achieving the optimal bound.¹⁵

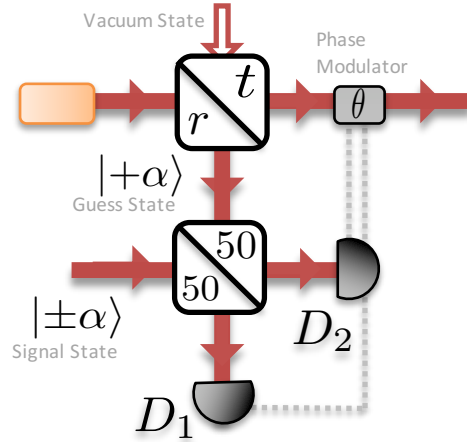


Figure 4. Schematics for the optimal USD-based amplifier for two states.

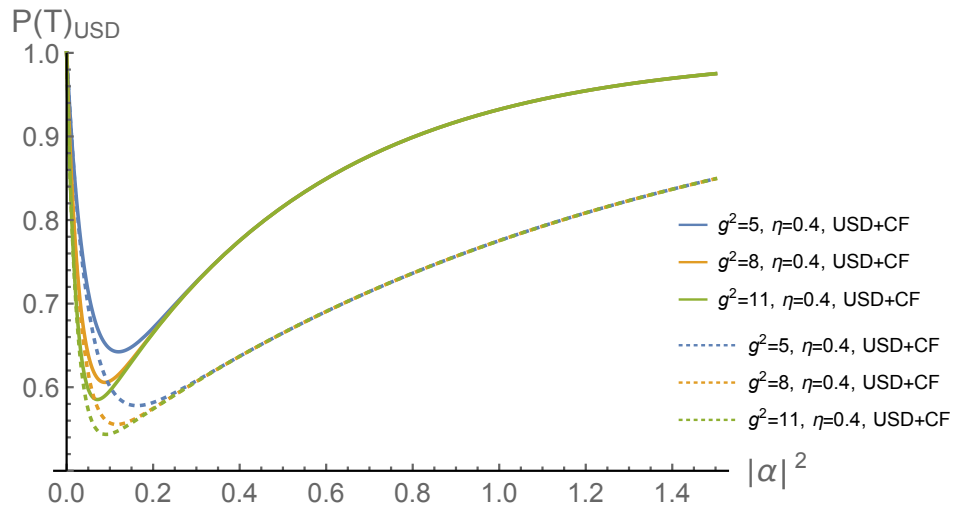


Figure 5. Success probability-fidelity product as a function of the input mean photon number for various values of the gain g^2 for the USD plus coin-flip. Solid lines (dashed) correspond to a detection efficiency of 1 (0.4).

It is natural to compare a USD based system with the SCAMP. Being unambiguous, the fidelity of a USD based system is always equal to one, at least in an ideal case that does not take into account unavoidable experimental imperfections such as dark counts and interferometer misalignment.

Here we compare the success probability-fidelity product. In order to carry out a fair comparison we have also considered a case when the USD based system is allowed, when inconclusive, to randomly flip a coin and output an amplified state, note that when no detector registers an event this is the best strategy as Bob has not gained any information about the input state, in this case the success probability is unity and the probability of passing a measurement test with the amplified output is given by:

$$P(T)_{USD} = P_{USD} + (1 - P_{USD}) \frac{1}{2} \left(1 + e^{-4g^2|\alpha|^2} \right). \quad (23)$$

The values of the fidelity-success probability product are plotted in figure 5, the general trend is similar to the SCAMP with feedforward state correction. For low mean photon numbers the "not triggering" events dominate and the output quality decreases as $|\alpha|^2$ increases. After a certain point, whose position depends on the gain and detection efficiency, $P(T, S)$ begins to recover and asymptotically it reaches one. Again, the turning point is reached for lower mean photon number as the gain increases but it corresponds to a deeper minimum. Also

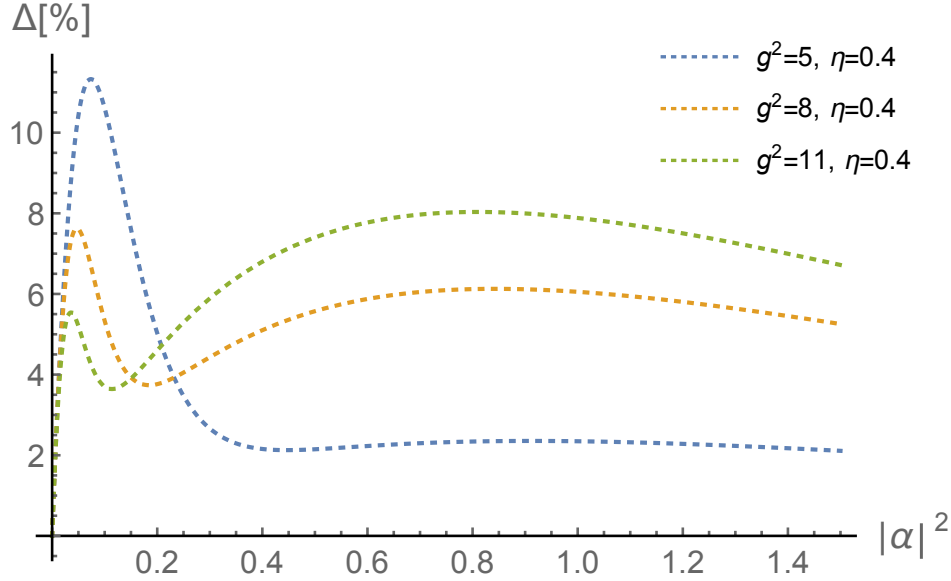


Figure 6. Percentage advantage of the feed-forward SCAMP with respect to the USD plus coin-flip as a function of the input mean photon number for various values of the gain g^2 .

in this case, the effect in the success probability-fidelity product of inefficient detection does not change this behaviour but it pushes the recovery to higher mean photon number as it decreases the probability of registering events at the detectors.

In figure 6 it is plotted the percentage advantage of the SCAMP with feedforward with respect to the USD plus coin-flip, i.e.:

$$\Delta = 100 \frac{P(T,S) - P(T)_{USD}}{P(T)_{USD}}. \quad (24)$$

In this plot we considered a detection efficient of 0.4 in order to present a real case scenario. The success probability-fidelity product of the SCAMP with feedforward state correction is always higher (up to 10%) than the one of the USD plus random output when inconclusive. The advantage is at least 2% for all the mean photon number considered.

5. CONCLUSIONS

We presented an high rate, high gain approximate probability amplifier with state correction based on feed-forward. The success probability-fidelity product of this device is always higher than the on of the USD plus random output when inconclusive.

This system can be realised with classical resources (i.e., lasers, linear optics and APD detectors). Similar systems, with no state correction, proved to achieve high-gain, high fidelity and high repetition rates^{16, 17} and¹⁸. The ability to switch between input states on the fly requires delay lines and fast switching but it can still achieved with classical resources.

Due to its simplicity, the system we propose might represent an ideal candidate as a recovery station to counteract quantum signal degradation due to propagation in a lossy fibre or as a quantum receiver. The system is also suitable for on-chip implementation.

APPENDIX A. AMPLITUDE CALCULATION

Here we compute the coherent amplitudes reaching the detectors in the outputs of the first and the second comparison beam splitters. If Bob's guess is right, i.e. Alice has chosen $|+\alpha\rangle$, we have that:

$$\begin{bmatrix} t_1 & r_1 \\ -r_1 & t_1 \end{bmatrix} \begin{bmatrix} \frac{t_1}{r_1} \alpha \\ \alpha \end{bmatrix} = \begin{bmatrix} \frac{\alpha}{r_1} \\ 0 \end{bmatrix}. \quad (25)$$

On the other hand if Bob's guess was wrong, i.e. Alice has chosen $|\alpha\rangle$, we have that:

$$\begin{bmatrix} t_1 & r_1 \\ -r_1 & t_1 \end{bmatrix} \begin{bmatrix} \frac{t_1}{r_1}\alpha \\ -\alpha \end{bmatrix} = \begin{bmatrix} \frac{t_1^2 - r_1^2}{r_1}\alpha \\ -2t_1\alpha \end{bmatrix}. \quad (26)$$

We can use the Kelly-Kleiner formula¹⁹ to compute the probability of a detection outcome. Assuming a detection efficiency of η_1 , we have that the probability of recording or not one event are respectively given by:

$$P(\mathbf{X}_1|\beta_1, +\alpha) = e^{-\eta_1|0|^2} = 1, \quad (27)$$

$$P(\mathbf{X}_1|\beta_1, -\alpha) = e^{-\eta_1|2t_1\alpha|^2}, \quad (28)$$

$$P(\check{\mathbf{X}}_1|\beta_1, +\alpha) = 1 - e^{-\eta_1|0|^2} = 0, \quad (29)$$

$$P(\check{\mathbf{X}}_1|\beta_1, -\alpha) = 1 - e^{-\eta_1|2t_1\alpha|^2}. \quad (30)$$

Let us now consider the second comparison beam splitter. If Bob's guess is right, we have that:

$$\begin{bmatrix} t_2 & r_2 \\ -r_2 & t_2 \end{bmatrix} \begin{bmatrix} \frac{t_2}{r_2 r_1}\alpha \\ \frac{\alpha}{r_1} \end{bmatrix} = \begin{bmatrix} \frac{\alpha}{r_2 r_1} \\ 0 \end{bmatrix}. \quad (31)$$

If Bob's guess is wrong and the first detector did not fired, we have that:

$$\begin{bmatrix} t_2 & r_2 \\ -r_2 & t_2 \end{bmatrix} \begin{bmatrix} \frac{t_2}{r_2^2 r_1^2}\alpha \\ \frac{t_1^2 - r_1^2}{r_1}\alpha \end{bmatrix} = \begin{bmatrix} \frac{1 - 2r_1^2 r_2^2}{r_1 r_2}\alpha \\ -2t_2 r_1 \alpha \end{bmatrix}. \quad (32)$$

On the other hand, if the first detector fires Bob can correct the out by using as second input the state $|\frac{1}{t_2} \left(\frac{-1 - r_2^2(t_1^2 - r_1^2)}{r_1 r_2} \right) \alpha\rangle$, in fact we have that:

$$\begin{bmatrix} t_2 & r_2 \\ -r_2 & t_2 \end{bmatrix} \begin{bmatrix} \frac{1}{t_2} \left(\frac{-1 - r_2^2(t_1^2 - r_1^2)}{r_1 r_2} \right) \alpha \\ \frac{t_1^2 - r_1^2}{r_1}\alpha \end{bmatrix} = \begin{bmatrix} -\frac{\alpha}{r_1 r_2} \\ \dots \end{bmatrix}. \quad (33)$$

Note that in this case the output of the second beam splitter is simply disregarded. We can thus compute the probability of the remaining events:

$$P(\mathbf{X}_2, \mathbf{X}_1|\beta_2, \beta_1, +\alpha) = e^{-\eta_1|0|^2} e^{-\eta_2|0|^2} = 1, \quad (34)$$

$$P(\mathbf{X}_2, \mathbf{X}_1|\beta_2, \beta_1, -\alpha) = e^{-\eta_1|2t_1\alpha|^2} e^{-\eta_2|2r_1 t_2 \alpha|^2}. \quad (35)$$

ACKNOWLEDGMENTS

The work was supported by the UK Quantum Technology Hub for Quantum Communications Technologies funded by UK Engineering and Physical Sciences Research Council (EP/M013472/1).

REFERENCES

- [1] Caves, C. M., "Quantum limits on noise in linear amplifiers," *Phys. Rev. D* **26**, 1817–1839 (Oct 1982).
- [2] Ralph, T. C. and Lund, A. P., "Nondeterministic noiseless linear amplification of quantum systems," *AIP Conference Proceedings* **1110**(1), 155–160 (2009).
- [3] Pandey, S., Jiang, Z., Combes, J., and Caves, C. M., "Quantum limits on probabilistic amplifiers," *Phys. Rev. A* **88**, 033852 (Sep 2013).
- [4] Eleftheriadou, E., Barnett, S. M., and Jeffers, J., "Quantum optical state comparison amplifier," *Phys. Rev. Lett.* **111**, 213601 (Nov 2013).
- [5] Chefles, A. and Barnett, S. M., "Optimum unambiguous discrimination between linearly independent symmetric states," *Physics Letters A* **250**(4), 223 – 229 (1998).

- [6] Bennet, C. H. and Brassard, G., “Quantum cryptography: Public key distribution and coin tossing,” *Proc. of IEEE Int. Conf. on Comp., Syst. and Signal Proc., Bangalore, India, Dec. 10-12, 1984* , 175–179 (1984).
- [7] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., “Quantum cryptography,” *Rev. Mod. Phys.* **74**, 145–195 (Mar 2002).
- [8] Campagna, M. and et al., [*Quantum Safe Cryptography and Security*], vol. 8, ETSI, 979-10-92620-03-0 (June 2015).
- [9] Mazzarella, L., Ticozzi, F., Sergienko, A. V., Vallone, G., and Villoresi, P., “Asymmetric architecture for heralded single-photon sources,” *Phys. Rev. A* **88**, 023848 (Aug 2013).
- [10] Branny, A., Kumar, S., Proux, R., and Gerardot, B., “Deterministic strain-induced arrays of quantum emitters in a two-dimensional semiconductor,” *Nature Communications* **8**, 15053 EP – (May 2017).
- [11] Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z., Tanaka, A., Yoshino, K., Nambu, Y., Takahashi, S., Tajima, A., Tomita, A., Domeki, T., Hasegawa, T., Sakai, Y., Kobayashi, H., Asai, T., Shimizu, K., Tokura, T., Tsurumaru, T., Matsui, M., Honjo, T., Tamaki, K., Takesue, H., Tokura, Y., Dynes, J. F., Dixon, A. R., Sharpe, A. W., Yuan, Z. L., Shields, A. J., Uchikoga, S., Legré, M., Robyr, S., Trinkler, P., Monat, L., Page, J.-B., Ribordy, G., Poppe, A., Allacher, A., Maurhart, O., Länger, T., Peev, M., and Zeilinger, A., “Field test of quantum key distribution in the tokyo qkd network,” *Opt. Express* **19**, 10387–10409 (May 2011).
- [12] Clarke, P., Collins, R., Dunjko, V., Andersson, E., Jeffers, J., and Buller, G., “Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light,” *Nature Communications* **3**, 1174 EP – (Nov 2012).
- [13] Donaldson, R. J., Collins, R. J., Kleczkowska, K., Amiri, R., Wallden, P., Dunjko, V., Jeffers, J., Andersson, E., and Buller, G. S., “Experimental demonstration of kilometer-range quantum digital signatures,” *Phys. Rev. A* **93**, 012329 (Jan 2016).
- [14] Buller, G. S. and Collins, R. J., “Single-photon generation and detection,” *Measurement Science and Technology* **21**(1), 012002 (2010).
- [15] Van Enk, S. J., “Unambiguous state discrimination of coherent states with linear optics: Application to quantum cryptography,” *Phys. Rev. A* **66**, 042313 (Oct 2002).
- [16] Usuga, M., Müller, C., Wittmann, C., Marek, P., Filip, R., Marquardt, C., Leuchs, G., and Andersen, U., “Noise-powered probabilistic concentration of phase information,” *Nature Physics* **6**, 767 EP – (Aug 2010).
- [17] Donaldson, R. J., Collins, R. J., Eleftheriadou, E., Barnett, S. M., Jeffers, J., and Buller, G. S., “Experimental implementation of a quantum optical state comparison amplifier,” *Phys. Rev. Lett.* **114**, 120505 (Mar 2015).
- [18] Donaldson, R. J., Mazzarella, L., Collins, R. J., Jeffers, J., and Buller, G. S., “A high gain, high fidelity and scalable quantum optical coherent state amplifier,” *In preparation* .
- [19] Kelley, P. L. and Kleiner, W. H., “Theory of electromagnetic field measurement and photoelectron counting,” *Phys. Rev.* **136**, A316–A334 (Oct 1964).