Feedforward-assisted coherent-state comparison amplifier

M. Bathaee, N. Marjan, and A. R. Bahrampour
Department of Physics, Sharif University of Technology, P.O. Box 11365-9161, Tehran, Iran

(Received 23 June 2019; published 8 October 2019)

Quantum optical coherent-state comparison amplifiers are nondeterministic devices which can amplify rather noiselessly a weak coherent state with an unknown phase from a finite discrete set. The high fidelity and high success probability of this amplifier are accomplished by a comparison stage and some photon subtraction stages. Due to the heralding nature of these amplifiers, they work part of the time. Here, we propose a feedforward protocol to increase the heralded times by correcting the incorrect guess. Hence, we enhance the fidelity and success probability more. Finally, the schematic experimental configuration of the feedforward-assisted coherent-state comparison amplifier is proposed.

DOI: 10.1103/PhysRevA.100.043809

I. INTRODUCTION

Amplifiers have made progress significantly after the invention of the maser in the 1950s and now they are used as one of the essentials in optical fiber communications. Classical signals such as the amplitude of electrical voltages can be increased rather arbitrarily whereas their signal-to-noise ratios (SNRs) are kept high. However, quantum mechanics laws prevent amplifying a quantum signal without decreasing its SNR. These quantum signals may be a coherent state which leads to the minimum uncertainty (shot noise) in electromagnetic quadratures [1]. In deterministically amplifying quantum signals, an additional noise is introduced which gives rise to the SNR reduction [2–4]. There is a connection between the introduced additional noise by quantum amplifiers and the no-cloning theorem [5]. In fact, based on quantum mechanics principles it is impossible to reduce deterministically the indistinguishability of two nonorthogonal states during amplification [6].

Apart from the importance of studying the amplification of a quantum signal from a quantum mechanics foundation viewpoint [2,7], the appearance of quantum computers urges us to utilize unconditional secure quantum communications which apply quantum amplifiers in long-distance communications [8,9]. So there is a high demand for amplification of a quantum signal such as in coherent states which are routinely employed in current quantum optical communication protocols [10,11] without introducing any additional noise. The noteworthy question is whether it is possible.

Generally, amplifiers can be characterized into two main groups: deterministic and nondeterministic amplifiers. Although any deterministic amplification leads to introducing an undesirable additional noise, nondeterministic amplifiers can circumvent this fundamental noise limit. The nondeterministic amplification can amplify a quantum signal perfectly by compromising the number of times that the output is successfully amplified. For example, an ideal deterministic phase-preserving linear amplifier launches at least an extra vacuum noise unit [7] whereas a nondeterministic noiseless linear amplifier (NLA) works partly yet perfectly [6,12]. The performance of hybridization of probabilistic and deterministic amplifiers has also been investigated [13,14].

The best practical NLAs are those that work without the need for any quantum resources and they can be implemented with linear optical devices. The quantum state comparison amplifiers (SCAMPs) are those which satisfy both aforementioned conditions [15,16]. Since in quantum optical communications such as quantum key distribution (QKD) protocols weak coherent pulses are mainly recruited for encoding information, SCAMPs are applicable in the implementation of these protocols. The SCAMP performs based on two main stages: state comparison and photon subtraction stages. In the former an unknown weak coherent pulse is compared to a guess via a beam splitter [17]. The destructive interference in one of the outputs of the beam splitter is determined by no photon detection in this stage. In the latter, another beam splitter will verify the quality of the final amplified output if any photon detection occurs in the reflected branch of the second beam splitter. So those outputs which are related to no-click and click situations of the detectors of the first and second beam splitters, respectively, are postselected. The corresponding probability of this situation is called the success probability. When the unknown weak signals come from a finite set, nonzero success probability can be achieved even for the amplified output with high fidelity [6]. Reference [16] showed that increasing the number of the photon subtraction stage enhances the amplified output fidelity as well.

In this paper, we enhance the success probability of the SCAMP by utilizing a feedforward mechanism. Since today's commercial single-photon detectors have a very low dark count, any photon detection in a comparison stage can be attributed to a wrong guess. Therefore, one can compare a next possible guess from the finite signal set with the output of the previous comparison stage again. This scheme needs a feedforward protocol which modifies the input of the next photon subtraction stage according to the next guess provided the previous detectors would have clicked. Thus this stage transforms to another comparison stage with a new guess. We show that this procedure leads to boosting both success probability and the fidelity of the SCAMP. The theoretical analysis and possibility of practical realization of our proposed feedforward scheme for a binary set and a set with N elements of unknown signals (a general case) are vigorously studied. A similar idea based on the feedforward state correction was proposed in Ref. [18]. However, they did not utilize photon subtraction in their feedforward scheme and they only considered a binary set amplification with a different strategy compared to our study.

This paper is organized as follows: In Sec. II, the idea of the feedforward mechanism is explained and it is studied for amplifying a signal coming from a binary set. The feedforward-assisted signal amplification from a set with cardinality N is generalized in Sec. III. Moreover, a practical feasible scheme for implementation of the feedforward-assisted amplifier is presented. Finally, the paper is concluded in Sec. IV.

II. FEEDFORWARD-ASSISTED METHOD

The SCAMPs are mainly based on comparing a weak coherent signal and a guess of the signal through their interference on a beam splitter, which is called the state comparison (SC) stage. One of the outputs of the beam splitter is a heralding branch which indicates whether the guess can be correct. No photon detection in this branch leads to a positive heralding result. The other output can be an amplified signal provided the heralding response is positive.

What can be concluded if the heralding response is negative? Considering a detector with no dark count, any photon detection in the heralded branch gives rise to the conclusion that the first guess was incorrect. Our feedforward-assisted SCAMPs are chiefly based on using a second guess for such cases and comparing it with the output result of the first comparison stage via another beam splitter.

In any ordinary SCAMPs there is another stage which increases the quality of the output. It is an important stage since a no-click on the SC detector is not a necessary consequence of the destructive interference between the correct guess and the signal. Loss, non-unite detector efficiency, and vacuum distribution in any coherent state can lead to no photon detection. This stage is called the photon subtraction (PS) stage which includes another beam splitter and a detector. Any detection in this detector can be a signature that the initial guess is more likely to be correct. Increasing the number of such stages enhances the fidelity of the amplified output. In our proposed feedforward-assisted SCAMP scheme, PS stages can be transformed to another SC stage based on the results of former detectors.

As a consequence, any feedforward-assisted SCAMP comprises a subsequence of beam splitters. One of the outputs of each beam splitter is terminated to a detector. Inputs of the first beam splitter are the weak coherent signal and the first guess. One of the inputs of the other beam splitters is always the output of the previous beam splitter. Based on the results of the previous detectors, the second input of each beam splitter is fed forward by the next new guess or a vacuum state.

For better clarification, in this section we explain the feedforward-assisted SCAMP where the weak coherent signals are chosen from a known binary set, i.e., $\{|\alpha\rangle, |-\alpha\rangle\}$, which is practical in some quantum communication protocols.

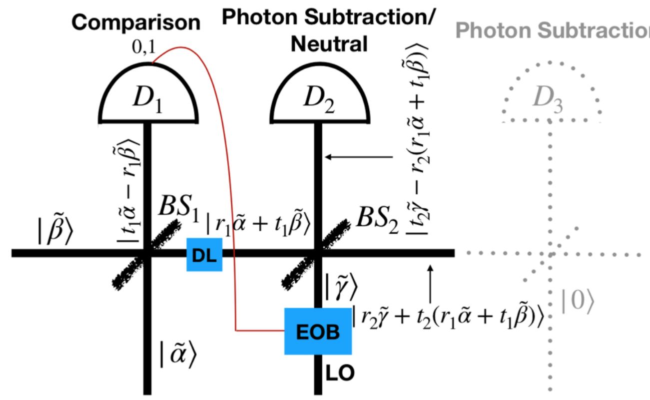

FIG. 1. The schematic configuration of the feedforward-assisted SCAMP for the binary set of signals. BS_i is the ith beam splitter. D_i is the ith detector. EOB is an electro-optical box which justifies proper amplitude and phase of the beam splitter input based on the D_1 result. LO is the preshared local oscillator between the transmitter and receiver. DL stands for a delay line. The thin red line is an electrical wire. The thick black lines are optical fibers.

QKD protocols can be implemented by weak coherent pulses where information is encoded in their relative phases [10]. For instance, in the B92 QKD protocol [19], a transmitter chooses randomly a quantum state from a binary set $\{|\alpha'\rangle, |-\alpha'\rangle\}$ where a classical bit 1(0) is encoded in the coherent state $|\alpha'\rangle(|-\alpha'\rangle)$. Then this quantum state is sent to the receivers. Due to the loss in quantum channels such as optical fibers, the amplitude of the signal decreases to $\alpha = \alpha' \exp(-a)$, where a is the measurable loss between the receiver and transmitter. Therefore, the receiver is aware that the received signal is randomly chosen from the binary set $\{|\alpha\rangle, |-\alpha\rangle\}$. Now, the receiver as a trusted node asks to amplify this weak coherent signal with unknown phase via our feedforward-assisted SCAMP scheme.

Figure 1 illustrates our proposed feedforward-assisted SCAMP. As it is shown in Fig. 1, the amplifier contains two beam splitters which are indicated by BS_1 and BS_2. Each beam splitter is respectively related to the SC and PS stages. A possible result of corresponding detectors can be $(D_1, D_2) \in \{(0, 1), (1, 0), (1, 1), (0, 0)\}$. In an ordinary SCAMP just the result (0,1) is postselected and others are removed. The feedforward mechanism enhances the performance of the amplifier by keeping the detector results $\{(1, 0), (1, 1)\}$. Assuming no dark count on detector D_1, if in the SC stage there is a detection, it is concluded that the first guess ($|\tilde{\beta}\rangle$) was incorrect. Since the unknown signals ($|\tilde{\alpha}\rangle$) are selected completely randomly from the binary set, the transmitter's strategy for choosing the first guess is preparing a coherent state with a proper proportion of the signal intensity, i.e., $|\frac{t_1}{r_1}\alpha|^2$, while its phase is randomly adjusted to one of the binary set states. For instance, the coherent state $|\frac{t_1}{r_1}\alpha\rangle$ is chosen as the first guess, where t_i (r_i) is the transmission (reflection) coefficient of BS_i. It is assumed that all beam splitters introduce a π phase to all reflected beams towards detectors. Therefore, the prepared coherent state $|\frac{t_1}{r_1}\alpha\rangle$ guarantees a destructive interference in the position of D_1 provided the guess is correct. On the other hand, when D_1 fires, it is concluded that the guess was wrong so the unknown signal state will be the second choice of the binary set. In our choice for the first guess ($|\frac{t_1}{r_1}\alpha\rangle$), when $D_1 = 1$ the signal will be $|-\alpha\rangle$. Since the demand is for the same output gain for all cases, the next stage for the case $D_1 = 1$ will be changed to the stage in which the amplified output is adjusted to a desired one. We call this stage the neutral stage. By inserting another proper input into BS_2 which is indicated by $|\tilde{\gamma}\rangle$ (see Fig. 1), the desired amplified output can be produced. The desired amplified output is $|\frac{t_2}{r_1}\tilde{\alpha}\rangle$ which is a perfect amplified output for the case $D_1 = 0$ and $D_2 = 1$ in an ordinary SCAMP. So the value of $\tilde{\gamma}$ depends on the D_1 results. Note that all variables which are governed by specific distributions are indicated by the tilde symbol.

In a nutshell, the overall amplifier has three inputs: the first guess $|\tilde{\beta}\rangle$, the unknown signal $|\tilde{\alpha}\rangle$, and the state which is modified based on the D_1 results, $|\tilde{\gamma}\rangle$. Accordingly, the outputs of the two subsequent stages are respectively $|t_1\tilde{\beta} + r_1\tilde{\alpha}\rangle$ and $|t_2(t_1\tilde{\beta} + r_1\tilde{\alpha}) + r_2\tilde{\gamma}\rangle$. Whenever the first detector results in $D_1 = 0$, the variable $\tilde{\gamma}$ is shown by γ_0 and it must be zero, which means the related input of the BS_2 is a vacuum state. So this stage becomes the PS stage in which the detector result related to $D_2 = 1$ is only postselected. On the other hand, if $D_1 = 1$, $\tilde{\gamma} = \gamma_1$ is determined such that the final output becomes $|\frac{t_2}{r_1}\tilde{\alpha}\rangle$. Therefore, this stage becomes the neutral stage. If the first guess is adjusted by $\tilde{\beta} = \frac{t_1}{r_1}\alpha$, whenever $D_1 = 1$, the signal must have been $|-\alpha\rangle$. Hence, by inserting $|\gamma_1\rangle = |-x\alpha\rangle$ where $x = t_2(t_1^2 + t_1^2)/(r_1 r_2)$ as the input of the BS_2, the desired amplified output $|-\frac{t_2}{r_1}\alpha\rangle$ is achieved. The related probability distributions of inputs $|\tilde{\alpha}\rangle$, $|\tilde{\beta}\rangle$, and $|\tilde{\gamma}\rangle$ are written respectively as

$$P(\tilde{\alpha}) = \frac{1}{2}\{\delta^2(\tilde{\alpha} - \alpha) + \delta^2(\tilde{\alpha} + \alpha)\},$$
$$Q(\tilde{\beta}) = \frac{1}{2}\{\delta^2(\tilde{\beta} - \beta) + \delta^2(\tilde{\beta} + \beta)\}, \quad \beta = \frac{t_1}{r_1}\alpha, \tag{1}$$
$$\Gamma_0(\tilde{\gamma}) = \delta^2(\tilde{\gamma}), \quad \Gamma_1(\tilde{\gamma}) = \delta^2(\tilde{\gamma} - \gamma_1),$$

where $\delta^2(x)$ is a two-dimensional Dirac delta function, $P(\tilde{\alpha})$ is the probability distribution of signals which are indicated randomly from the binary set $\{|\alpha\rangle, |-\alpha\rangle\}$ by the transmitter, and $Q(\tilde{\beta})$ is the probability distribution of guesses which are chosen randomly from the binary set $\{|\beta\rangle, |-\beta\rangle\}$ by the receiver. The probability distribution Γ_{D_1} is specified according to the result of the first detector by the transmitter.

The probability that detectors resulting in (D_1, D_2) conditioning the inputs are coherent states $|\tilde{\alpha}\rangle$, $|\tilde{\beta}\rangle$, and $|\tilde{\gamma}\rangle$ is indicated by $\mathcal{P}(D_1, D_2|\tilde{\alpha}, \tilde{\beta}, \tilde{\gamma})$. Since in the postselection the situation where two detectors are off is discarded, $P(0, 0|\tilde{\alpha}, \tilde{\beta}, \tilde{\gamma}) = 0$. If η_i is the efficiency of the ith detector, the probability of any photon detection (no photon detection) in the detector with coherent input $|c_i\rangle$ is determined in line with $p(D_i = 1|c_i) = 1 - \exp(\eta_i|c_i|^2)$ [$p(D_i = 0|c_i) = \exp(\eta_i|c|^2)$] [20]. Therefore, $\mathcal{P}(D_1, D_2|\tilde{\alpha}, \tilde{\beta}, \tilde{\gamma}) = p(D_1|c_1)p(D_2|c_2)$, where c_i is a function of $\tilde{\alpha}$, $\tilde{\beta}$, and $\tilde{\gamma}$. As a result, the total success probability given the case (0,0) is removed in the postselection can be written in the following form:

$$P_S(|\alpha|) = \sum_{D_1, D_2} \iiint d^2\tilde{\alpha} d^2\tilde{\beta} d^2\tilde{\gamma} \times P(\tilde{\alpha})Q(\tilde{\beta})\Gamma_{D_1}(\tilde{\gamma})\mathcal{P}(D_1, D_2|\tilde{\alpha}, \tilde{\beta}, \tilde{\gamma}). \tag{2}$$

The addition of the cases (1,0) and (1,1) is the direct signature of the success probability enhancement of the feedforward scheme. The fidelity of the output of the final beam splitter for any specific variables $\tilde{\alpha}$, $\tilde{\beta}$, and $\tilde{\gamma}$ relative to the desired amplified state $|\frac{t_2}{t_1}\tilde{\alpha}\rangle$ is called the fidelity test. Since the fidelity test depends on the value of D_1, it is indicated by T_{D_1} and accordingly is defined by

$$T_0 = \left|\langle t_2(t_1\tilde{\beta} + r_1\tilde{\alpha})\middle|\frac{t_2}{r_1}\tilde{\alpha}\rangle\right|^2,$$
$$T_1 = 1. \tag{3}$$

$T_1 = 1$ due to the fact that in the binary set space of signals the second guess reveals the unknown signal. Hence, the amplifier performs perfectly for this situation. Indeed T_{D_1} is the probability that the output state collapses to the desired amplified state, i.e., $|\frac{t_2}{r_1}\tilde{\alpha}\rangle$. It is clear that the fidelity test is a function of $\tilde{\alpha}$, $\tilde{\beta}$, and $\tilde{\gamma}$. To avoid cluttering, these parameters are removed. As a result the overall fidelity of the amplifier corresponding to the output passing the fidelity test provided the results of the detectors are acceptable in the postselection is defined by

$$F(T|S; |\alpha|) = \frac{P(S, T; |\alpha|)}{P_S(|\alpha|)},$$
$$P(S, T; |\alpha|) = \sum_{D_1, D_2} \iiint d^2\tilde{\alpha} d^2\tilde{\beta} d^2\tilde{\gamma} \tag{4}$$
$$\times P(\tilde{\alpha})Q(\tilde{\beta})\Gamma_{D_1}(\tilde{\gamma})\mathcal{P}(D_1, D_2|\tilde{\alpha}, \tilde{\beta}, \tilde{\gamma})T_{D_1},$$

where $P(S, T; |\alpha|)$ is the probability that the system passes the fidelity test in addition to the setup operating successfully. The successful operation is related to the acceptable heralding situation of the feedforward-assisted amplifier. Demanding higher fidelity for the case (0,1), another photon subtraction stage can be added to the amplifier [16]. On the one hand, any detection in the second PS stage can be a signature that the higher input intensity must have gone through the third beam splitter (blurred beam splitter shown in Fig. 1). Therefore, no photon detection in the SC stage is more probable to be related to the destructive interference of the guess and signal. Hence, the guess is more likely to be the correct one. On the other hand, adding beam splitters with transmission coefficients less than 1 leads to a decrease of the output gain. As a result, there is a trade-off between increasing the gain and fidelity. It is obvious that when the heralding conditions grow, with increasing PS stages, the success probability decreases.

When the signal comes from a set with three possible states, this third beam splitter can lead to the enhancement of the success probability and the fidelity through correcting all wrong guesses in the previous stages via the feedforward mechanism compared to the ordinary SCAMP with two PS stages. Please note that in this paper we focus on utilizing a different number of PS stages in favor of increasing the number of possible unknown signals which can be better amplified according to the feedforward mechanism compared to the ordinary counterpart. More explanation of the generalized feedforward-assisted SCAMP is presented in Sec. III.

III. GENERALIZED FEEDFORWARD MECHANISM

As mentioned before, any SCAMP has two kinds of subsequent modular stages: a state comparison (SC) stage and multiple photon subtraction (PS) stages. Each stage interferes two coherent-state inputs on a beam splitter and they result in two outputs. One of the outputs impinges on a detector as a heralding result and the other is supposed to be an amplified output of an unknown signal. There is a trade-off between increasing the fidelity and decreasing the gain of the output by increasing the number of PS stages. However, these stages can be utilized to correct the incorrect initial guess state occurring in the SC stage through a feedforward procedure, which is the goal of this paper.

Our suggested feedforward strategy alters some of the PS stages to the SC stage based on the results of the detectors. As illustrated in Ref. [16], in the SCAMP without the feedforward mechanism, the SC stage inputs comprise an unknown signal and a guessed state, whereas in the PS stage, the output of previous stages and a vacuum state are inputs. Furthermore, in the SC stage there must exist no click in its related detector while in the PS stages their related detectors must click; accordingly the final output is postselected. The proposed feedforward mechanism starts playing its role whenever there is a detection in the SC stage. Assuming detectors have no dark count, the three following modifications must occur in the subsequent stages of the original SCAMP after firing in the SC detector:

First, the stage after this stage changes to the other SC stage. This new SC stage compares the unknown output of the previous stage, which is a combination of the unknown signal and all previous guessed states, with a new guess.

Second, since this stage is transformed to the SC stage, one of its inputs that used to be fed by a vacuum state must be modified appropriately according to the next possible guessed state. The proper input for this level is chosen such that, if the next guessed state is correct, the detector of this stage never clicks.

Third, whenever any PS stage transforms to the SC stage due to the feedforward mechanism, the last PS stage must provide the same amplified output as the other cases. It happens by replacing its vacuum input with the coherent state prepared properly based on all the previous guesses. So, the detection results of the last PS stage become inconclusive. We call this stage the neutral stage. In the postselection process both possible results of the final detector ($D_N \in \{0, 1\}$) are kept.

The quality of the fidelity is examined again by the following PS stages after any new SC stage. In the following sections, respectively, first the methodology of the generalized feedforward-assisted amplifier is investigated and then a related experimental setup for such a system is proposed.

A. Methods

Similar to hitherto suggested SCAMPs, the feedforward-assisted SCAMP performs effectively where weak signals belong to a predetermined finite set [6]. So, in this paper it is assumed that signals are weak coherent pulses from a finite set with a known fixed amplitude ($|\alpha|$) and their relative phases

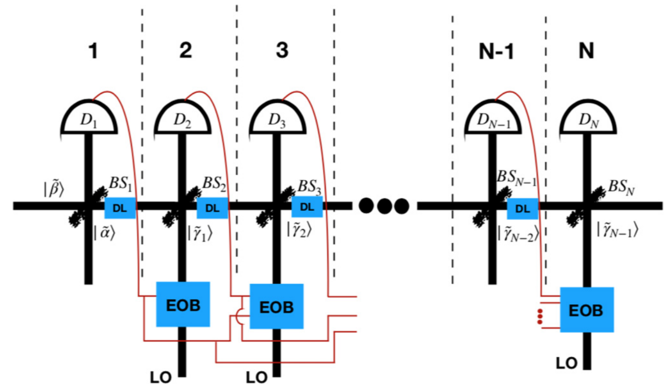

FIG. 2. Schematic configuration of the generalized feedforward-assisted SCAMP. Blue boxes indicated by EOB are a combination of an amplitude and a phase modulator which modulate the local oscillator based on the logical bits that arise by outputs of previous detectors. The thin red lines are electrical wires and thick black lines are optical fibers. DL stands for delay line.

are discretized based on a uniform distribution in the phase spaces (the limited discrete-phase alphabet) as follows:

$$|\alpha_i\rangle = ||\alpha|e^{i\phi_i}\rangle \;\; \phi_i \in \Phi = \left\{0, \frac{2\pi}{N}, \dots, \frac{2\pi(N-1)}{N}\right\}, \qquad (5)$$

where N determines the number of possible signals. The schematic configuration of the generalized feedforward-assisted SCAMP is depicted in Fig. 2.

As shown in Fig. 2, the first stage is always the state comparison stage with two inputs: a weak coherent unknown signal $|\tilde{\alpha}\rangle$ and a properly prepared first guessed state $|\tilde{\beta}\rangle$. Considering signals uniformly selected from the predefined set of Eq. (5), $|\tilde{\alpha}\rangle$ and $|\tilde{\beta}\rangle$ have the following distributions:

$$P(\tilde{\alpha}) = \frac{1}{N}\sum_{i=1}^{N}\delta^2(\tilde{\alpha} - \alpha_i),$$

$$Q(\tilde{\beta}) = \frac{1}{N}\sum_{i=1}^{N}\delta^2(\tilde{\beta} - \beta_i), \;\; \beta_i = \frac{t_1}{r_1}\alpha_i, \qquad (6)$$

where t_i and r_i are, respectively, the transmission and reflection coefficients of the ith beam splitter. Click and no click on the detectors are indicated by 1 and 0, respectively. Hence a sequence $(D_1, D_2 \dots, D_N)$, where $D_i \in \{0, 1\}$, specifies different scenarios for the feedforward mechanism. For instance, $(0, 1, 1, \dots, 1)$ (one zero and $N-1$ ones) is the only postselected result in the original SCAMP. As mentioned in the first part of this section, in any comparison stage, if the corresponding detector clicks, the next stage will transform to a new comparison stage in which the next guessed state compares to the output of the previous stage. Assuming $D_1 = 1$, therefore, the output of the first beam splitter (BS_1) $|t_1\tilde{\beta} + r_1\tilde{\alpha}\rangle$ must interfere with $|\tilde{\gamma}_1\rangle$ in the next beam splitter (BS_2) such that if the second guess of the unknown signal is correct, $D_2 = 0$. Without loss of generality, we illustrate the ith guessed state by $|\bar{\alpha}_i\rangle$. Note that the phase of $\bar{\alpha}_i$ is randomly chosen from the set Φ [see Eq. (5)]. As a result, $\tilde{\gamma}_1 = \frac{r_2}{t_2}(r_1\bar{\alpha}_2 + t_1\tilde{\beta})$, where $\tilde{\beta} = \frac{t_1}{r_1}\bar{\alpha}_1$ and $|\bar{\alpha}_2\rangle$ is the second chosen guess. Since $\bar{\alpha}_2 \neq \bar{\alpha}_1$, the phase difference ($\Delta\phi_i^{(1)}$)

between variables $\bar{\alpha}_2$ and $\bar{\alpha}_1$ belongs to the set $\Delta\Phi^{(1)}$ with cardinality $N-1$, which is specified by

$$\Delta\phi_i^{(1)} \in \Delta\Phi^{(1)} = \left\{\frac{2\pi}{N}, \frac{4\pi}{N}, \dots, \frac{2(N-1)\pi}{N}\right\}. \quad (7)$$

Consequently, the related distribution of $\tilde{\gamma}_1$ is

$$\Gamma^{(1)}_{D_1=1}(\tilde{\gamma}_1) = \frac{1}{N-1}\sum_{i=1}^{N-1}\delta^2(\tilde{\gamma}_1 - \gamma_1^i),$$
$$\gamma_1^i = \frac{r_2}{t_2}\tilde{\beta}\left(\frac{r_1^2}{t_1}e^{i\Delta\phi_i^{(1)}} + t_1\right). \quad (8)$$

It is clear that if $D_1 = 0$, $\Gamma^{(1)}_{D_1=0}(\tilde{\gamma}_1) = \delta^2(\tilde{\gamma}_1)$, which means $|\tilde{\gamma}_1\rangle = |0\rangle$. In general, the distribution of $\tilde{\gamma}_i$ depends on all the previous detector results. The next stages after this new SC stage remain the PS stage whenever $D_2 = 0$. Since it is required to reach the same gain for all possible and acceptable detector outcomes, $|\tilde{\gamma}_{N-1}\rangle$, the upward input of the neutral stage, the final beam splitter (see Fig. 2), must be prepared such that the desired amplified output $|(t_2t_3\cdots t_N/r_1)\tilde{\alpha}\rangle$ is accomplished. In the case where $D_1 = 1$, $D_2 = 0$, and all the other detectors except D_N must fire [i.e., $(1, 0, 1, \dots, 1, 0)$ or $(1, 0, 1, \dots, 1, 1)$], $\tilde{\gamma}_{N-1}$ is uniquely determined according to $\bar{\alpha}_1$ and $\bar{\alpha}_2$ as follows:

$$\Gamma^{(N-1)}_{1,0,1,\dots,1}(\tilde{\gamma}_{N-1}) = \delta^2(\tilde{\gamma}_{N-1} - \gamma_{N-1}),$$
$$\gamma_{N-1} = \frac{1}{r_N}\left[\frac{t_N\cdots t_2}{r_1}\bar{\alpha}_2 - t_N\cdots t_3 \times (t_2(t_1\tilde{\beta} + r_1\bar{\alpha}_2) + r_2\tilde{\gamma}_1)\right],$$
$$\bar{\alpha}_2 = \frac{1}{t_1}\left(\frac{t_2}{r_2}\tilde{\gamma}_1 - t_1\tilde{\beta}\right). \quad (9)$$

In the neutral stage both click and no click of D_N are counted in the postselection. Please note that all the detectors after D_2 except D_N must fire since they are related to the PS stages.

If $D_1 = 1$ and $D_2 = 1$, the second guess has been also incorrect provided there is no dark count. As a consequence, the next stage will be another SC stage which contains the third guess. Now, $|\tilde{\gamma}_2\rangle$ must be prepared based on the third guessed state $\bar{\alpha}_3$ as well as the two previous guesses $\bar{\alpha}_1$ and $\bar{\alpha}_2$ such that $\bar{\alpha}_1 \neq \bar{\alpha}_2 \neq \bar{\alpha}_3$ and $D_3 = 0$ if the third guess is correct. The number of possibilities for $\bar{\alpha}_3$ is $N-2$. If $\bar{\phi}_1$ and $\bar{\phi}_2$ are respectively the corresponding phases of $\bar{\alpha}_1$ and $\bar{\alpha}_2$, $\bar{\phi}_3$ belongs to the set $\Phi - \{\bar{\phi}_1, \bar{\phi}_2\}$. Hence, the probability distribution of $\tilde{\gamma}_2$ provided $(D_1 = 1, D_2 = 1)$ is given by

$$\Gamma^{(2)}_{D_1=1D_2=1}(\tilde{\gamma}_2) = \frac{1}{N-2}\sum_{j=1}^{N-2}\delta^2(\tilde{\gamma}_2 - \gamma_2^j), \quad (10)$$

where

$$\gamma_2^j = \frac{r_3}{t_3}\left[t_2\left(t_1\tilde{\beta} + r_1\bar{\alpha}_3^j\right) + r_2\tilde{\gamma}_1\right], \quad (11)$$

$\tilde{\gamma}_1$ is determined based on the probability distribution of Eq. (8), $\bar{\alpha}_3^j = \bar{\alpha}_1 e^{i\Delta\phi_j^{(2)}}$, $\Delta\phi_j^{(2)} = \bar{\phi}_3^j - \bar{\phi}_1$, and $\bar{\phi}_3^j \in \Phi - \{\bar{\phi}_1, \bar{\phi}_2\}$ for every j. This process will continue in the same manner. For example, as mentioned in Sec. II where $N = 2$,

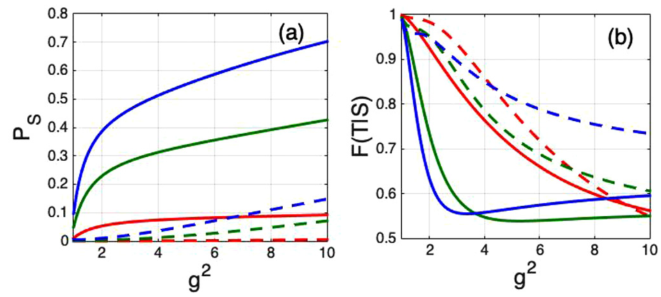

FIG. 3. The (a) success probability and (b) fidelity of the SCAMP with $N = 3$ versus intensity gain $g^2 = |t_2t_3/r_1|^2$ with (without) the feedforward mechanism indicated by solid (dashed) lines for three different signal intensities $|\alpha|^2 = 0.1, 0.5, 1$, which are depicted by red, green, and blue, respectively. In these curves, (0,1,1), (1,0,1), (1,0,0), (1,1,0), and (1,1,1) are the results of the detectors which are postselected. The efficiency of all detectors is assumed $\eta_i = 1/2$ and transmission coefficients of the second and third beam splitters are assumed to be fixed to 90%.

(D_1, D_2) can be (0,1), (1,0), (1,1), and (0,0). Our feedforward procedure yields the output for the first three cases and only (0,0) is discarded in the postselection. Moreover, in the case (1,0) and (1,1), the output is the same as the desired one which is $|\frac{t_2}{r_1}\tilde{\alpha}\rangle$. In general, it is straightforward to show that the feedforward mechanism applied in a SCAMP with N beam splitters saves detector results in the form of $(11\cdots1011\cdots1x)$, where x (the last beam splitter result) can be both 0 and 1. The sign $\cdots$ stands for some replications of 1 before and after the detector that has not fired. Hence, in addition to the case $(011\cdots1)$, the number of $2(N-1)$ results will be added to the postselection of the feedforward-assisted SCAMP which increases the success probability. However, some of these cases can hurt the overall fidelity compared to the ordinary SCAMP without the feedforward mechanism with one SC and $N-1$ PS stages. It is due to the fact that the feedforward-assisted SCAMP for these cases is transformed to the ordinary SCAMP with $N-(n+2)$ PS stages, where n is the number of detectors that they have clicked before the detector with no click. Figure 3 illustrates the fidelity reduction of our feedforward strategy compared to the ordinary SCAMP for the case $N = 3$ with two PS stages where we have kept the detector results $\{(0, 1, 1), (1, 0, 1), (1, 0, 0), (1, 1, 0), (1, 1, 1)\}$ from all possible results corresponding to three detectors. The cases $(1, 0, 1)$ and $(1, 0, 0)$ happen when the first guess is wrong but the second guess has a chance to be correct. Since for these cases the third stage is responsible for adjusting the gain value to the desired one, i.e. $g = t_2t_3/r_1$, this neutral stage has no effect on the fidelity or success probability. As a result, the amplifier for these cases behaves as if it is a SCAMP without a PS stage for the unknown signal set with cardinality 2 which degrades the fidelity compared to the SCAMP with PS stages.

Since the enhancement of the output fidelity is requested, we omit cases which can be seen as the detector results of an ordinary SCAMP with a reduced number of PS stages from the postselection.

So in any generalized feedforward-assisted SCAMP only two other detector results $(11\cdots10)$ (all detectors except the

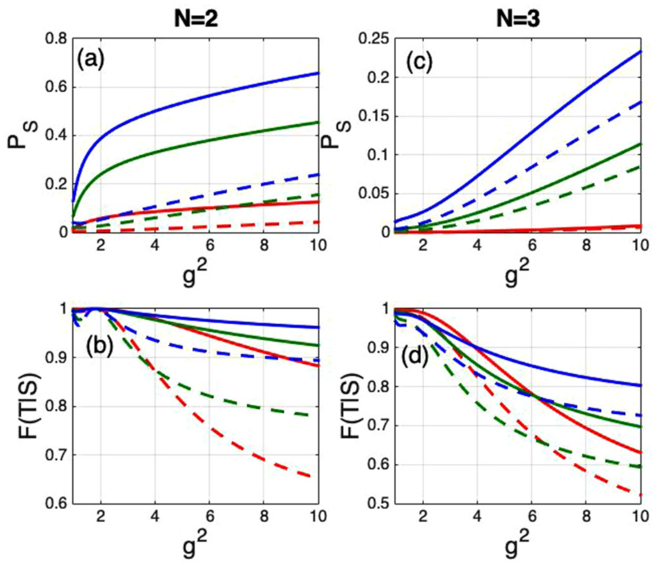

FIG. 4. The (a, c) success probability and (b, d) fidelity of the SCAMP with (without) feedforward mechanism as functions of intensity gain which are indicated by solid (dashed) lines for three different signal intensities $|\alpha|^2 = 0.1, 0.5, 1$, which are depicted by red, green, and blue, respectively: (a, b) binary set with intensity gain $g^2 = |t_2/r_1|^2$; (c), (d) $N = 3$ with intensity gain $g^2 = |t_2 t_3/r_1|^2$ where only the detector results of (0,1,1), (1,1,0), and (1,1,1) are postselected. The efficiency of all detectors is assumed $\eta_i = 1/2$ and the transmission coefficients of the second and third beam splitters are fixed to 90%.

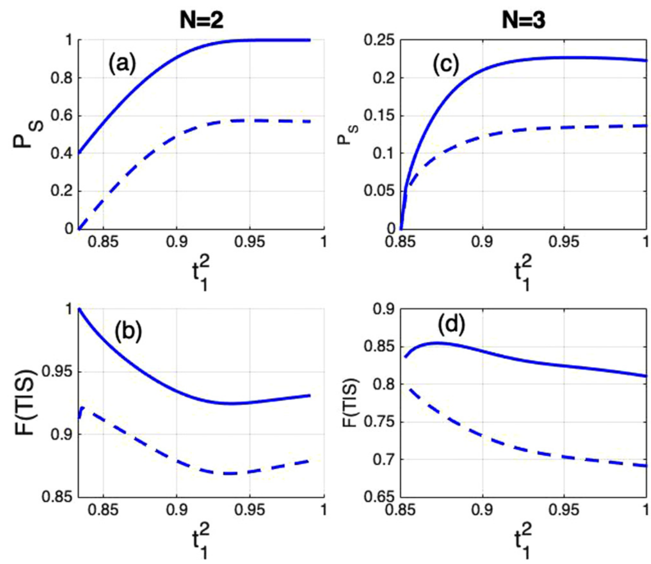

FIG. 5. The (a, c) success probability and (b, d) fidelity of the SCAMP with (without) feedforward mechanism as functions of transmission coefficient t_1^2 which are indicated by solid (dashed) lines for the signal intensity $|\alpha|^2 = 1$: (a, b) binary set with the fixed intensity gain $g^2 = |t_2/r_1|^2 = 6$; (c, d) $N = 3$ with the fixed intensity gain $g^2 = |t_2 t_3/r_1|^2 = 6$ where only the detector results of (0,1,1), (1,1,0), and (1,1,1) are postselected. The efficiency of all detectors is assumed $\eta_i = 1/2$ and transmission coefficients of the third beam splitters are fixed to 90%.

last one fire) and $(11\cdots 11)$ (all detectors fire) will be added to the postselection, which leads to the correct guess and thus a perfect amplification will occur. Nevertheless, these two cases are enough to see a rather considerable enhancement in the output fidelity (see Fig. 4).

All in all, the feedforward-assisted SCAMP has $N+1$ inputs which are $|\tilde{\beta}\rangle, |\tilde{\alpha}\rangle, |\tilde{\gamma}_1\rangle, \ldots, |\tilde{\gamma}_{N-1}\rangle$. Their related probability distributions of $|\tilde{\gamma}_i\rangle$ depend on the outcomes of the previous detectors. Therefore, one can write the success probability of this system as

$$P_S(|\alpha|) = \sum_{D_1,\ldots,D_N} \int \cdots \int d^2\bar{\alpha} d^2\bar{\beta} d^2\bar{\gamma}_1 \cdots d^2\bar{\gamma}_{N-1} \times P(\tilde{\alpha}) Q(\tilde{\beta}) \Gamma^1_{D_1}(\tilde{\gamma}_1) \cdots \Gamma^{N-1}_{D_1\cdots D_{N-1}}(\tilde{\gamma}_{N-1}) \times P(D_1 \cdots D_N | \tilde{\beta}, \tilde{\alpha}, \tilde{\gamma}_1, \ldots, \tilde{\gamma}_{N-1}), \tag{12}$$

where $P(D_1 \cdots D_N | \tilde{\beta}, \tilde{\alpha}, \tilde{\gamma}_1, \ldots, \tilde{\gamma}_{N-1})$ is the probability that the detector outcomes are $(D_1 \cdots D_N)$ provided the inputs are $(\tilde{\beta}, \tilde{\alpha}, \tilde{\gamma}_1, \ldots, \tilde{\gamma}_{N-1})$. It is important to note that the probabilities corresponding to all the cases which have been thrown away in the postselection must be set to zero in the summation of Eq. (12). Since the fidelity of the output for specific values of $(\tilde{\beta}, \tilde{\alpha}, \tilde{\gamma}_1, \ldots, \tilde{\gamma}_{N-1})$ is a function of detector outcomes [i.e., $T_{D_1,\ldots,D_N}(\tilde{\beta}, \tilde{\alpha}, \tilde{\gamma}_1, \ldots, \tilde{\gamma}_{N-1})$], the overall fidelity for all possible cases given that the setup operates successfully is written

$$F(T|S; |\alpha|) = \frac{P(T, S; |\alpha|)}{P_S(|\alpha|)}, \tag{13}$$

where

$$P(T, S; |\alpha|) = \sum_{D_1,\ldots,D_N} \int \cdots \int d^2\bar{\alpha} d^2\bar{\beta} d^2\bar{\gamma}_1 \cdots d^2\bar{\gamma}_{N-1} \times P(\tilde{\alpha}) Q(\tilde{\beta}) \Gamma^1_{D_1}(\tilde{\gamma}_1) \cdots \Gamma^{N-1}_{D_1\cdots D_{N-1}}(\tilde{\gamma}_{N-1}) \times P(D_1 \cdots D_N | \tilde{\beta}, \tilde{\alpha}, \tilde{\gamma}_1, \ldots, \tilde{\gamma}_{N-1}) \times T_{D_1,\ldots,D_N}(\tilde{\beta}, \tilde{\alpha}, \tilde{\gamma}_1, \ldots, \tilde{\gamma}_{N-1}) \tag{14}$$

is the probability that both the fidelity test $T_{D_1,\ldots,D_N}$ is passed and the setup successfully operates. The fidelity test can be calculated by $T = |\langle t_N \cdots t_2/r_1 \tilde{\alpha} | \text{output}\rangle|^2$ where $|\text{output}\rangle$ is the real final output of the SCAMP. For example, $T_{11\cdots 11} = T_{11\cdots 10} = 1$ due to the fact that all $N-1$ previous guesses have been wrong so the unknown signal state is revealed and the known state could be amplified without introducing any noise. Figures 4(a) and 4(c) and Figs. 4(b) and 4(d) depict, respectively, the enhanced performance of the feedforward mechanism for the success probability and fidelity versus the intensity gain $g^2 = (\frac{t_2\cdots t_N}{r_1})^2$ for three different $|\alpha|^2 = 0.1, 0.5, 1$. Figures 4(a) and 4(b) and Figs. 4(c) and 4(d) are respectively related to $N = 2$ and $N = 3$. Comparing Figs. 4(a) and 4(b) with Figs. 4(c) and 4(d), it is important to note that the feedforward mechanism enhances the performance of the SCAMP for a fixed N whereas increasing N gives rise to fidelity and success probability reductions akin to the ordinary SCAMP. Figure 5 illustrates how increasing the transmission coefficient of the first beam splitter given the intensity gain is constant can change the fidelity and success probability for both schemes $N = 2$ and $N = 3$, where $g^2 = 6$ and $|\alpha|^2 = 1$. As shown in Fig. 5 and as it would be predicted, the success

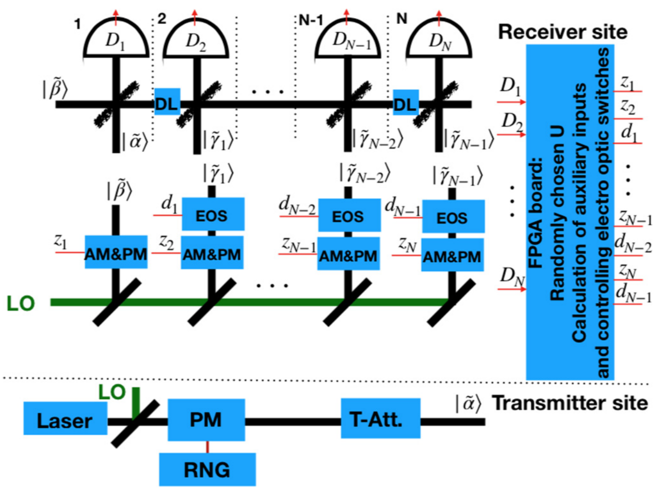

FIG. 6. A proposed experimental realization of the feedforward-assisted SCAMP. The thin red lines are related to electrical wires. The thick black and green lines are optical fibers. DL, delay line; PM, phase modulator; AM, amplitude modulator; LO, local oscillator; RNG, random number generator; EOS, electro-optic switch; T-Att models all kinds of attenuation between two sites. z_i gives proper electrical information to the AM and PM based on the randomly chosen set U to prepare the set $\tilde{\Gamma}$. d_i orders the EOS to be on and off based on the results of $(D_1, \dots, D_{i-1})$.

probability increases while fidelity decreases over t_1^2. If $t_1 = 1, r_1 = 0$. Therefore, the gain of intensity cannot remain 6 and any result related to this situation is meaningless.

B. The proposed experimental setup

In this section we investigate the possibility of the experimental realization of the feedforward-assisted SCAMP. Figure 6 depicts a schematic configuration of the experimental setup where the signals are chosen from the set with cardinality N. Since the information is encoded in the phase of the coherent state, sharing a reference phase dubbed local oscillator (LO) between a legitimate transmitter and receiver is mandatory.

The transmitter generates a coherent state via a laser source. A beam splitter provides the LO and the signal from the laser source. By use of a phase modulator (PM) accompanied by a random number generator (RNG), the transmitter prepares the signal with a random phase from the set Φ [see Eq. (5)]. Since the indistinguishability of possible outputs of the PM is crucial in the security of any QKD protocols, the signal is attenuated and then it is sent to the other party site, the receiver. The weak coherent signal and the strong LO are transported to the receiver site through two optical fibers. All kinds of losses including optical fiber loss are modeled by an attenuator which is indicated by "T-Att." in Fig. 6.

As mentioned in the previous section the ordered set $\tilde{\Gamma} = \{|\tilde{\beta}\rangle, |\tilde{\gamma}_1\rangle, \dots, |\tilde{\gamma}_{N-1}\rangle\}$ is determined by random guesses from the ordered signal set $S = \{|\alpha_1\rangle, \dots, |\alpha_N\rangle\}$ and results of detectors $D = \{D_1, \dots, D_N\}$. For the sake of simple implementation, we assume the receiver predetermines the subsequent guesses needed for preparing $|\tilde{\beta}\rangle$ and $|\tilde{\gamma}_i\rangle$ (called auxiliary inputs) before receiving each signal. The predetermined ordered guess set is an arbitrary randomly chosen permutation ($\mathcal{P}$) of the signal set, i.e., $U = \mathcal{P}S = \{u_1, \dots, u_N\}$ where $u_i \in S$. A field-programmable gate array (FPGA) board can provide different U through a RNG. It is important to note that randomly selecting the guess set for each signal guarantees that the final shared key between transmitter and receiver contains a rather equal number of 0s and 1s. By considering all different scenarios for the set D, all possible sets for $\tilde{\Gamma}$ are prepared according to the predetermined set U before receiving the signal. Each $\tilde{\gamma}_i$ is constructed by use of amplitude and phase modulators as well as the shared LO. The distinct scenarios for the set D are as follows:

(I) $D^{(1)} = \{0, 1, 1, \dots, 1\}$ where … stands for replication of 1. In this case $\tilde{\beta} = t_1/r_1 u_1$ and for all $i = 1, \dots, N-1$, $\gamma_i = 0$.

(II) $D^{(2)} = \{1, 1, \dots, 0\}$ or $D^{(2)} = \{1, 1, \dots, 1\}$. This happens when all detectors except the last one must fire. In these cases the system could recognize that all previous $N-1$ guesses have been wrong. Therefore, the last guess u_N is the same as the signal. Again $\tilde{\beta} = t_1/r_1 u_1$ but each $|\tilde{\gamma}_i\rangle$ is a function of first $i+1$ guesses $(u_1, \dots, u_{i+1})$ such that a destructive inference would have occurred in the port into the D_{i+1} if the guess u_{i+1} had been correct. For instance, Eq. (8) defines the explicit form of $\tilde{\gamma}_1$, where index i in this formula indicates a different permutation of guesses.

From scenarios I and II, it is clear that for each permutation of guesses there exist two possibilities for value of each $\tilde{\gamma}_i$. So, implanting an EOS performing based on the results of the detectors $(D_1, \dots, D_i)$ in the ith branch (stage) is necessary.

(III) $D^{(3)} = \{1, \dots, 1, 0, 1, \dots, 1\}$ where there are x number of 1s before and y number of 1s after 0. These cases are related to the situations when the feedforward mechanism transforms the original SCAMP with $N-1$ PS stages to the one with y PS stages. Depending on the appearance position of 0, it must be prepared with different $\tilde{\gamma}_{N-1}$ which includes $N-1$ different values. Since these cases decrease the overall fidelity of the feedforward-assisted SCAMP in comparison with the original one, we dismiss these cases from the postselection [see Fig. 3(b)].

Both detectors and modulators have finite rates. Therefore, a delay line must be placed between two stages [ith and $(i+1)$th] to keep the output of BS_i as long as the feedforward procedure decides and prepares a proper state for $\tilde{\gamma}_i$. An ordinary single photon detector such as ID210 from IDQ company [21] can have an order of nanosecond response time. Moreover, greater than gigahertz modulators are easily found in any market. As a result with a rough estimation, the delay line length is on the order of a centimeter. A high-speed FPGA board can accelerate any electrical processing according to the detector results.

It is noteworthy to mention that the setup with N beam splitters can be also utilized for amplifying weak signals randomly chosen from the set with cardinality less than N. In this case, all the extra beam splitters play the role of the photon subtraction stages which can be another way of fidelity enhancement. This modification must be considered when the FPGA board is being programmed.

Since the dark count and photon detection due to the nonvacuum state are independent events, the probability that the detector in the ith SC stage, D_i, fires while it has not been due to the dark count is the multiplication of $p(D_i = 1)$ (probability that the ith detector without dark count, D_i, clicks) and $1 - p_{\rm Dark}$. As a result, the destructive effect of the nonzero dark count rate can be included in our calculation via multiplying each term of Eq. (12) or Eq. (14) which is related to the photon detection in D_i by $1 - p_{\rm Dark}$. For current commercial single photon detectors such as IDQ210, the dark count rate can be a few hertz for a repetition rate of 100 kHz [21]. Therefore, the dark count probability $p_{\rm Dark}$ is on the order of 10^{-5}. Hence, we neglect this effect in our calculation.

IV. CONCLUSION

We improve the performance of the quantum coherent state comparison amplifier (SCAMP) through the feedforward mechanism. First, we have shown how the feedforward protocol can enhance the success probability and fidelity of the SCAMP with practically important signals of a binary set. We have shown our scheme can be easily generalized to any finite number set of weak coherent signals. The enhancement of the success probability and fidelity of the feedforward-assisted SCAMP for two special cases $N = 2$ and $N = 3$ versus the amplifier gain has been numerically illustrated and compared. Finally, we have investigated a practical feasible scheme for an implementation of the feedforward-assisted SCAMP.

[1] C. Gerry, P. Knight, and P. L. Knight, *Introductory Quantum Optics* (Cambridge University Press, Cambridge, U.K., 2005).
[2] C. M. Caves, Phys. Rev. D **26**, 1817 (1982).
[3] P. K. Lam, T. C. Ralph, E. H. Huntington, and H. A. Bachor, Phys. Rev. Lett. **79**, 1471 (1997).
[4] V. Josse, M. Sabuncu, N. J. Cerf, G. Leuchs, and U. L. Andersen, Phys. Rev. Lett. **96**, 163602 (2006).
[5] U. L. Andersen, V. Josse, and G. Leuchs, Phys. Rev. Lett. **94**, 240503 (2005).
[6] S. Pandey, Z. Jiang, J. Combes, and C. M. Caves, Phys. Rev. A **88**, 033852 (2013).
[7] C. M. Caves, J. Combes, Z. Jiang, and S. Pandey, Phys. Rev. A **86**, 063802 (2012).
[8] H. M. Chrzanowski, N. Walk, S. M. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul, and P. K. Lam, Nat. Photonics **8**, 333 (2014).
[9] D. Bai, P. Huang, H. Ma, T. Wang, and G. Zeng, Entropy **19**, 546 (2017).
[10] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[11] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[12] H. Adnane, F. Albarelli, A. Gharbi, and M. G. Paris, arXiv:1901.07480.
[13] J. Y. Haw, J. Zhao, J. Dias, S. M. Assad, M. Bradshaw, R. Blandino, T. Symul, T. C. Ralph, and P. K. Lam, Nat. Commun. **7**, 13222 (2016).
[14] J. Combes, N. Walk, A. P. Lund, T. C. Ralph, and C. M. Caves, Phys. Rev. A **93**, 052310 (2016).
[15] E. Eleftheriadou, S. M. Barnett, and J. Jeffers, Phys. Rev. Lett. **111**, 213601 (2013).
[16] R. J. Donaldson, L. Mazzarella, R. J. Collins, J. Jeffers, and G. S. Buller, Commun. Phys. **1**, 54 (2018).
[17] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).
[18] L. Mazzarella, R. J. Donaldson, R. J. Collins, U. Zanforlin, G. Tatsi, G. S. Buller, and J. Jeffers, *Quantum Technologies 2018* (SPIE, Bellingham, WA, 2018), Vol. 10674, p. 106741D.
[19] P. K. Verma, M. El Rifai, and K. W. C. Chan, *Multi-photon Quantum Secure Communication* (Springer, Berlin, 2019), pp. 59–84.
[20] P. Kelley and W. Kleiner, Phys. Rev. **136**, A316 (1964).
[21] https://www.idquantique.com/single-photon-systems/products/id210/.