

## Boosting linear-optical Bell measurement success probability with predetection squeezing and imperfect photon-number-resolving detectors

Thomas Kilmer and Saikat Guha

College of Optical Sciences, University of Arizona, Tucson, Arizona 85721, USA



(Received 29 September 2018; published 1 March 2019)

Linear-optical realizations of Bell state measurement (BSM) on two single-photon qubits succeed with probability  $p_s$  no higher than 0.5. However, predetection quadrature squeezing, i.e., quantum noise limited phase sensitive amplification, in the usual linear-optical BSM circuit, can yield  $p_s \approx 0.643$ . The ability to achieve  $p_s > 0.5$  has been found to be critical in resource-efficient realizations of linear-optical quantum computing and all-photonic quantum repeaters. Yet, the aforesaid value of  $p_s > 0.5$  is not known to be the maximum achievable using squeezing, thereby leaving it open whether close-to-100% efficient BSM might be achievable using squeezing as a resource. In this paper, we report insights on why squeezing-enhanced BSM achieves  $p_s > 0.5$ . Using this, we show that the previously reported  $p_s \approx 0.643$  at single-mode squeezing strength  $r = 0.6585$ —for unambiguous state discrimination (USD) of all four Bell states—is an experimentally unachievable point result, which drops to  $p_s \approx 0.59$  with the slightest change in  $r$ . We, however, show that squeezing-induced boosting of  $p_s$  with USD operation is still possible over a continuous range of  $r$ , with an experimentally achievable maximum occurring at  $r = 0.5774$ , achieving  $p_s \approx 0.596$ . Finally, deviating from USD operation, we explore a trade space between  $p_s$ , the probability with which the BSM circuit declares a “success,” versus the probability of error  $p_e$ , the probability of an input Bell state being erroneously identified given the circuit declares a success. Since quantum error correction could correct for some  $p_e > 0$ , this tradeoff may enable better quantum repeater designs by potentially increasing the entanglement generation rates with  $p_s$  exceeding what is possible with traditionally studied USD operation of BSMs.

DOI: [10.1103/PhysRevA.99.032302](https://doi.org/10.1103/PhysRevA.99.032302)

### I. INTRODUCTION

In the so-called *dual-rail* photonic qubit basis, the logical qubits  $|0\rangle$  and  $|1\rangle$  are realized by one photon in one of two orthogonal modes (while the other mode is in vacuum). Two common physical realizations are (1) one photon in one of two orthogonal polarization modes (of a single spatiotemporal mode), i.e.,  $|0\rangle = |1\rangle_H$  and  $|1\rangle = |1\rangle_V$ ; and (2) one photon in one of two orthogonal spatial modes (of the same polarization), i.e.,  $|0\rangle = |10\rangle$  and  $|1\rangle = |01\rangle$ . In this paper we will consider the latter form of the dual-rail photonic qubit basis.

The four Bell states form a complete orthonormal basis for two qubits. Each is a maximally entangled state of two qubits, representing 1 ebit of shared entanglement. Equations (1) are the four 2-qubit four-mode Bell states in the dual-rail encoding, where the mode pairs 1 and 2, and 3 and 4 each represent one qubit.

$$|\psi_+\rangle = \frac{1}{\sqrt{2}}(|1001\rangle + |0110\rangle), \quad (1a)$$

$$|\psi_-\rangle = \frac{1}{\sqrt{2}}(|1001\rangle - |0110\rangle), \quad (1b)$$

$$|\phi_+\rangle = \frac{1}{\sqrt{2}}(|1010\rangle + |0101\rangle), \quad (1c)$$

$$|\phi_-\rangle = \frac{1}{\sqrt{2}}(|1010\rangle - |0101\rangle). \quad (1d)$$

Projecting a pair of qubits onto the Bell basis is an important primitive in quantum computation and communication.

This two-qubit projective measurement is often termed the Bell basis measurement, or the Bell state measurement (BSM). Uses of BSMs include quantum teleportation [1,2], entanglement swapping [3], dense coding [4], quantum repeaters [5,6], and fault-tolerant quantum computing [2,7].

It has been long known that if the optical circuit used to realize a BSM on two dual-rail qubits is restricted to using passive linear-optical elements (beam splitters and phase shifters), the BSM can succeed with at most 50% success probability [8]. This probabilistic nature of the linear-optical BSM has arguably been the primary bottleneck in realizing scalable all-photonic quantum computing [7,9] and other all-photonic quantum information processing, such as all-photonic quantum repeaters for long-distance entanglement distribution [10,11], where an entangled cluster state of several photons in a “code state” mimics the action of a quantum memory by providing error correction against photon loss.

#### A. Boosted Bell state measurements

The success probability ( $p_s$ ) of a BSM circuit is the probability with which it can unambiguously identify a randomly assigned Bell state presented to the circuit as input. When restricted to passive linear optics and no ancillary states, one cannot achieve  $p_s > 50%$  [8]. However, it was recently shown that including predetection quadrature squeezing and photon-number-resolving (PNR) detection (along with linear optics) can boost (increase)  $p_s$  to  $\sim 64.3%$  [12]. Further, it was also recently found that the addition of unentangled single-photon

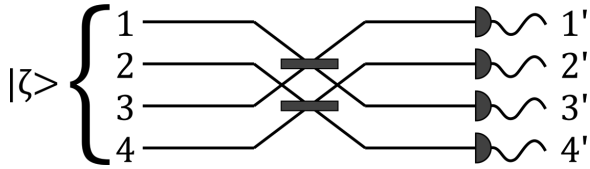


FIG. 1. The optical circuit that identifies a randomly input Bell state  $|\zeta\rangle \in \{|\psi_+\rangle, |\psi_-\rangle, |\phi_+\rangle, |\phi_-\rangle\}$  with success probability  $p_s = 0.5$ . With probability  $1 - p_s = 0.5$ , it produces an erasure (“I don’t know”) outcome. This is an example of unambiguous state discrimination (USD).

ancillae and PNR detection (along with linear optics) can boost  $p_s$  to up to 78.125% [13]. The addition of arbitrarily large entangled ancillae and PNR detection (along with linear optics) can boost  $p_s$  to 100% [14].

Any quantum measurement on a set of  $n$  linear-optical qubits can be realized by a suitable  $2n$ -mode quantum unitary transformation followed by ideal PNR detectors. A *universal* set of optical transformations is one from which one can draw elements to build an arbitrary unitary transformation on any set of optical modes. One example of a universal set comprises the following subsets: (1) passive linear-optical elements (circuits involving beam splitters and phase shifters) and on-off detectors [15], (2) squeezing [realized, e.g., using an optical parametrical amplifier (OPA) built using a  $\chi^{(2)}$  non-linear-optical material], and (3) PNR detectors. The most general multimode *Gaussian* transformation is one that can be built by drawing elements from subsets (1) and (2) [16]. Adding any one non-Gaussian element—which can be either (a) a non-Gaussian nonlinear *transformation* such as the Kerr or cubic phase, (b) a non-Gaussian ancilla *state* such as single photons or cat states, or (c) a non-Gaussian *measurement* such as PNR detection—to the set of Gaussian transformations makes it a universal set [17]. The linear-optical circuit for BSM that achieves  $p_s = 50\%$  (shown in Fig. 1) involves elements only from the subset (1) above. In fact, one cannot exceed this success probability with a  $2n$ -mode circuit comprised of elements drawn from (1) alone [8].

Since optical elements from (1), (2), and (3) above form a universal set, a BSM circuit must exist that uses linear optics, squeezing, and PNR detectors that achieves  $p_s = 100\%$ . The boosted BSM circuit proposed by Zaidi and van Loock [12] that achieves  $p_s \approx 64.3\%$  employs exactly those elements (linear optics, squeezing, and PNR detectors). This circuit is shown in Fig. 2. The universality of the elements used in realizing this circuit, and the practical realizability of inline squeezing and PNR detection [18] are the reasons we will

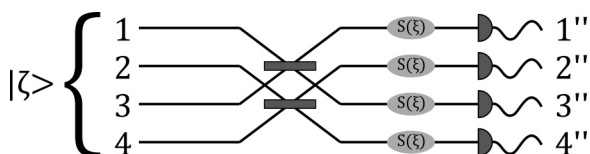


FIG. 2. An optical circuit which can identify unambiguously a randomly input Bell state  $|\zeta\rangle \in \{|\psi_+\rangle, |\psi_-\rangle, |\phi_+\rangle, |\phi_-\rangle\}$  with  $p_s > 50\%$ .  $S(\xi)$  represents a single-mode squeezer (e.g., an OPA), where  $\xi = \frac{1}{2}e^{i\phi}\tanh r$  is the degree of squeezing.

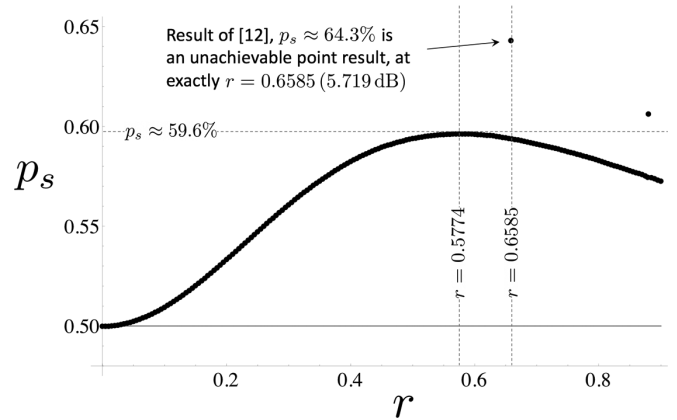


FIG. 3. Bell measurement success probability ( $p_s$ ) vs squeezing intensity ( $r$ ) for a squeezed Bell measurement circuit.

study boosted BSM using predetection squeezing in further detail, in this paper.

## B. Main results

The main results of this paper are summarized below.

(1) We review the squeezing-boosted BSM circuit in Ref. [12] and provide a deeper understanding and intuition for why it boosts  $p_s$  beyond the 50% limit of linear optics without ancillae.

(2) We show that the  $p_s \approx 64.3\%$  result of [12] is actually a point result achievable with a predetection squeezing of *exactly* 5.719 dB (squeezing parameter,  $r = 0.6585$ ) in all four squeezers in the circuit in Fig. 2. If the applied squeezing in any of the squeezers is even infinitesimally lower or higher than that,  $p_s$  drops (discontinuously) to a lower value, but it stays strictly higher than 50% (see Fig. 3).

(3) We evaluate the effect of finite photon-number resolution in the PNR detectors. We find that (1) at least three-photon resolving detectors are needed to get any boost of  $p_s$  above 50%, specifically  $p_s \approx 0.54$  being achievable with three-photon-resolving PNR detectors and 3 dB of squeezing ( $r \approx 0.35$ ); (2) most of the nondiscontinuous boost in  $p_s$  possible from predetection squeezing,  $\approx 59\%$ , can be obtained with seven-photon-resolving PNR detectors (e.g., recently demonstrated transition edge sensor (TES) detectors by National Institute of Standards and Technology [18]).

(4) In all of the existing research on boosted linear optic BSMs [8,12–14], the definition of *success* of a BSM is based on the so-called unambiguous state discrimination (USD) framework, where one demands that when one of the four Bell states is presented to the BSM circuit at random, if the circuit does produce a result identifying the input as one of the four Bell states, it is 100% certain that a particular Bell state was input. With probability  $1 - p_s$ , it produces an “I don’t know” (erasure) outcome.

With imperfect (subunity detection efficiency, nonzero dark click rate) PNR detectors, even the BSM circuits in Refs. [8,12–14] will *not* produce a USD outcome and cannot be analyzed as such. Further, in certain applications, it may be advantageous to trade a higher “success” probability  $p_s$ , the probability the circuit produces some nonerasure result,

with a nonzero “error” probability ( $p_e$ ), the probability that the produced measurement result is incorrect (for USD,  $p_e = 0$ ).

In this paper we study the performance of predetection-squeezing-boosted BSM in such a non-USD, probabilistic state discrimination (PSD) framework, and work out the trade space between  $p_s$  and  $p_e$ . We also incorporate nonideal (subunity efficiency) PNR detection into this analysis.

## II. PASSIVE LINEAR OPTICS

The four Bell states (1) are mutually orthogonal quantum states, and hence perfectly and deterministically distinguishable by an appropriate quantum measurement. However, if all four modes of a (randomly) presented Bell state are detected using on-off detectors or PNR detectors, the Bell states are perfectly *indistinguishable*. This is because none of the four possible photon-number detection patterns  $(N_1, N_2, N_3, N_4) \in \{1001, 0110, 1010, 0101\}$  can uniquely identify the input Bell state, where  $N_i$  is the number of photons detected in mode  $i$ . The four 4-mode product number states  $\{|1001\rangle, |0110\rangle, |1010\rangle, |0101\rangle\}$  are each present in two Bell states. So the observation of a given number state does not uniquely identify a particular Bell state. Therefore, the USD BSM success probability achieved by direct PNR detection is  $p_s = 0\%$ .

However, the use of beam splitters prior to detecting the four modes, as shown in Fig. 1 can improve  $p_s$  to the 50% limit achievable with passive linear optics [8]. In this paper we will define a “beam splitter” to always refer to the following 50-50 beam splitter (2):

$$\begin{pmatrix} a_k^\dagger \\ a_l^\dagger \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} a_k^\dagger \\ a_l^\dagger \end{pmatrix}. \quad (2)$$

$$S(\xi)|n\rangle = \left( \frac{1}{\cosh(2r)} \right)^{n+1/2} (n!)^{1/2} \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{(-\xi^*)^j [\cosh(2r)]^{2j}}{(n-2j)!j!} \sum_{k=0}^{\infty} \frac{\xi^k [(n-2j+2k)!]^{1/2}}{k!} |n-2j+2k\rangle, \quad (4a)$$

$$\xi \equiv \frac{1}{2} e^{i\phi} \tanh r, \quad (4b)$$

$$\text{dB} = -10 \log_{10} (e^{-2r}). \quad (4c)$$

Assuming identical squeezing intensity  $r$  and rotation  $\phi = 0$  for each mode, the output states of the circuit in Fig. 2 for the four input Bell states are given in Eqs. (5). Note that these double-primed transformed Bell states are squeezing applied on the single-primed transformed states (3) at the output of the standard linear-optical BSM circuit in Fig. 1. Appendix B goes into greater detail about why we choose  $r$  and  $\phi$  to be the same for all four modes.

Let us note from Eq. (4) that squeezing is a parity-conserving operation, which maps a number state  $|n\rangle$  to an infinite superposition of all number states of like parity, i.e., if  $n$  is odd (respectively, even),  $S(\xi)|n\rangle$  is a superposition of all odd (respectively, even) number states. Additionally, let us define the parity of a set of modes in a product number state as the list of parities of the number of photons in each of those modes. For example, the parities of the (four-mode) number state components in  $|\psi'_+\rangle$  are (odd, odd, even, even) and (even, even, odd, odd), whereas the parity of the number state components in  $|\psi'_-\rangle$  are (odd, even, even, odd) and (even, odd, odd, even).

$$\begin{aligned} |\psi''_+(r)\rangle = & \frac{i(\text{sech } r)^4}{\sqrt{2}} |1100\rangle + \frac{i(\text{sech } r)^4}{\sqrt{2}} |0011\rangle + \frac{i(\text{sech } r)^4 \tanh r}{2} |0211\rangle + \frac{i(\text{sech } r)^4 \tanh r}{2} |2011\rangle \\ & + \frac{i(\text{sech } r)^4 \tanh r}{2} |1120\rangle + \frac{i(\text{sech } r)^4 \tanh r}{2} |1102\rangle + \frac{i(\text{sech } r)^4 (\tanh r)^2}{2} |1122\rangle + \dots, \end{aligned} \quad (5a)$$

Mixing modes 1 and 3, and 2 and 4 of the input Bell state on two beam splitters as shown in Fig. 1, produces the following output states:

$$|\psi'_+\rangle = \frac{i}{\sqrt{2}} (|1100\rangle + |0011\rangle), \quad (3a)$$

$$|\psi'_-\rangle = \frac{1}{\sqrt{2}} (|1001\rangle - |0110\rangle), \quad (3b)$$

$$|\phi'_+\rangle = \frac{i}{2} (|2000\rangle + |0020\rangle + |0200\rangle + |0002\rangle), \quad (3c)$$

$$|\phi'_-\rangle = \frac{i}{2} (|2000\rangle + |0020\rangle - |0200\rangle - |0002\rangle). \quad (3d)$$

The four output states in (3) are still mutually orthogonal and perfectly distinguishable as were the original input Bell states, since the two beam splitters comprise a unitary (and hence reversible) transformation. However, with on-off detection or PNR detection on these output states,  $p_s = 0.5$ . In order to see why, note that  $|\psi'_+\rangle$  and  $|\psi'_-\rangle$  are completely distinguishable with photon detection, while  $|\phi'_+\rangle$  and  $|\phi'_-\rangle$  remain wholly indistinguishable. Therefore, if one of the four Bell states is presented randomly (i.e., each with probability 1/4), the circuit in Fig. 1 will unambiguously identify the input state with average probability 50%. This circuit provides the framework for all subsequent *boosted* BSM circuits we will examine in this paper.

## III. PREDETECTION SQUEEZING

Zaidi and van Loock’s BSM circuit functions by applying predetection single-mode quadrature squeezing to each of the four output modes of the standard  $p_s = 50\%$  BSM circuit [12], as shown in Fig. 2. The action of single-mode squeezing  $S(\xi)$ , a unitary (hence, reversible) operation, on the number state  $|n\rangle$  is given by [19]

$$\begin{aligned}
|\psi''_-(r)\rangle = & \frac{(\operatorname{sech} r)^4}{\sqrt{2}}|0110\rangle - \frac{(\operatorname{sech} r)^4}{\sqrt{2}}|1001\rangle + \frac{(\operatorname{sech} r)^4 \tanh r}{2}|0112\rangle + \frac{(\operatorname{sech} r)^4 \tanh r}{2}|2110\rangle \\
& - \frac{(\operatorname{sech} r)^4 \tanh r}{2}|1021\rangle - \frac{(\operatorname{sech} r)^4 \tanh r}{2}|1201\rangle + \frac{(\operatorname{sech} r)^4 (\tanh r)^2}{2\sqrt{2}}|2112\rangle + \dots,
\end{aligned} \tag{5b}$$

$$\begin{aligned}
|\phi''_+(r)\rangle = & -i\sqrt{2}(\operatorname{sech} r)^2 \tanh r |0000\rangle - \frac{i(\operatorname{sech} r)^4 (\cosh(2r) - 2)}{2}|2000\rangle - \frac{i(\operatorname{sech} r)^4 (\cosh(2r) - 2)}{2}|0200\rangle \\
& - \frac{i(\operatorname{sech} r)^4 (\cosh(2r) - 2)}{2}|0020\rangle - \frac{i(\operatorname{sech} r)^4 (\cosh(2r) - 2)}{2}|0002\rangle + \dots,
\end{aligned} \tag{5c}$$

$$\begin{aligned}
|\phi''_-(r)\rangle = & \frac{i(\operatorname{sech} r)^4}{2}|2000\rangle - \frac{i(\operatorname{sech} r)^4}{2}|0200\rangle + \frac{i(\operatorname{sech} r)^4}{2}|0020\rangle - \frac{i(\operatorname{sech} r)^4}{2}|0002\rangle \\
& + \frac{i(\operatorname{sech} r)^4 \tanh r}{\sqrt{2}}|2020\rangle - \frac{i(\operatorname{sech} r)^4 \tanh r}{\sqrt{2}}|0202\rangle + \frac{i(\operatorname{sech} r)^4 (\tanh r)^2}{4}|2220\rangle + \dots
\end{aligned} \tag{5d}$$

Since single-mode squeezing on a number state is parity preserving, squeezing on a set of modes in a product number state is also parity preserving (by our definition of parity of a set of modes). Therefore, squeezing has no effect on the distinguishability of number state products that have unique parity. For example, the parities of the states of  $|\psi'_+\rangle$  and  $|\psi'_-\rangle$  remain unchanged after applying squeezing, and hence  $|\psi''_+\rangle$  and  $|\psi''_-\rangle$  remain perfectly distinguishable by PNR detection on all four modes regardless of the amount of squeezing applied. However, number states with like parity signatures, such as those of  $|\phi'_+\rangle$  and  $|\phi'_-\rangle$ , the parity of all the number states within which is (even, even, even, even), are mapped to an overlapping set of number states, each with (even, even, even, even) parity.

Even though  $|\phi'_+\rangle$  and  $|\phi'_-\rangle$  were completely indistinguishable by PNR detection, some distinguishability emerges between the postsqueezed states  $|\phi''_+\rangle$  and  $|\phi''_-\rangle$ . There are two distinct ways in which such distinguishability comes about:

(1) For all values of  $r$ , certain new number states, e.g.,  $\{|0000\rangle, |2002\rangle, |0220\rangle, \dots\}$ , appear in  $|\phi''_+\rangle$  but not in  $|\phi''_-\rangle$ , and vice versa. The detection of one of these states by PNR detection thus boosts  $p_s$  beyond 50%, while maintaining USD distinguishability. The probability of occurrence of these distinguishing states, and thus the boost in  $p_s$ , is a function of  $r$  (see Fig. 3).

(2) For certain discrete values of  $r$ , one or more of the states  $\{|2000\rangle, |0200\rangle, |0020\rangle, |0002\rangle, \dots\}$ , which  $|\phi'_+\rangle$  and  $|\phi'_-\rangle$  are both comprised of, interfere completely destructively for  $|\phi''_+\rangle$  but not for  $|\phi''_-\rangle$ , or vice versa. This produces additional USD distinguishability. However, this happens only for certain singular values of  $r$  and thus produces discontinuous boosts to  $p_s$  (see the two black dots in Fig. 3).

We performed a numerical calculation of the average distinguishability between the four Bell states, the details of which are given in Appendix A 3. The result, a plot of BSM success probability  $p_s$  as a function of squeezing intensity  $r$  (squeezing phase  $\phi = 0$ ) is shown in Fig. 3.

Reference [12] reported the measurement success peak at  $r = 0.6585$  (5.719 dB of squeezing), where  $p_s = 64.3\%$ . This peak occurs when  $\cosh(2r) - 2 = 0$ , causing the  $|2000\rangle, |0200\rangle, |0020\rangle$ , and  $|0002\rangle$  number states to destructively interfere within  $|\phi''_+\rangle$ , making them unique to  $|\phi''_-\rangle$ .

This adds an additional 4.94% success probability. There are infinitely many such discontinuous peaks in  $p_s$  at different values of  $r$  but this particular peak is the only one worth considering, as it occurs at the lowest  $r$ , has the highest relative increase in  $p_s$ , and has the highest absolute  $p_s$  of any such peak.

Unfortunately these peaks only exist for infinitesimally thin slices of  $r$ . They are discontinuous jumps in success probability and are not reasonable targets for USD measurements, as any uncertainty in  $r$  will cause the number states in question to become indistinguishable with PNR detection. Further attention will be given to these peaks later, when considering PSD measurements.

However, despite those discontinuous peaks, what is interesting is that along the entire continuous portion of the  $p_s$  vs  $r$  curve in Fig. 3, for every value of  $r$ , USD BSM is possible at  $p_s > 50\%$ . This contribution to the continuous boost in  $p_s$  comes from the squeezed number states that are perfectly distinguishable for all values of  $r$ . Considering only these universally distinguishable states, we find a maximum success probability of  $p_s = 59.6\%$  at  $r = 0.5774$  (5.015 dB of squeezing).

### A. Finite photon number resolution

Squeezing a number state produces an infinite sum (superposition) of number states with arbitrarily large photon numbers. However, existing state-of-the-art PNR detectors, the so-called TES detectors, cannot efficiently resolve number states with more than seven photons [18]. Using such detectors in the squeezing-boosted BSM circuit will truncate the number states beyond a certain number, which should be taken into consideration when evaluating the success probability. Figure 4 shows the  $p_s$  curves for a squeezed BSM circuit with PNR detectors limited to a maximum photon-number resolution ( $n_{\max}$ ) of 12 or fewer photons. These curves are compared to the  $p_s$  curve with arbitrarily high photon-number resolution.

Reasonably sized arrays of on-off detectors can be used to emulate the performance of PNR detectors for small photon numbers [20], which could be a more experimentally accessible realization of PNR detection than TES detectors for most

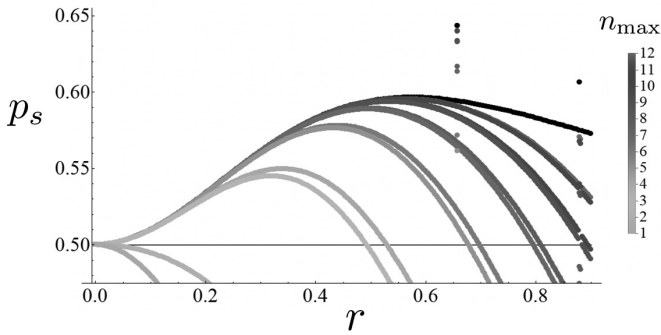


FIG. 4. Bell measurement success probability ( $p_s$ ) vs squeezing intensity ( $r$ ) for a predetection-squeezed BSM circuit, and with PNR detectors with maximum number resolution  $n_{\max} \in \{1, 2, \dots, 12\}$ . The case of  $n_{\max} = \infty$  from Fig. 3 is also shown for comparison (top black curve).

laboratories. However, in practice even small arrays of on-off detectors greatly increase the number of photon-number states. The computational resources required to characterize such systems increase exponentially with array size. We believe such an analysis may not be infeasible, but is beyond our reach given the computational resources at our disposal.

PNR detectors limited to  $n_{\max} = 7$  show a (discontinuous) success probability peak  $p_s = 61.3\%$  at  $r = 0.6585$  (5.719 dB of squeezing) and a continuous maxima of  $p_s = 58.9\%$  at  $r = 0.496$  (4.311 dB of squeezing).

### B. Probabilistic state discrimination

So far we have limited our analysis to USD, where one demands that when one of the four Bell states is presented to the BSM circuit at random, if the circuit does produce a result identifying the input as one of the four Bell states, it is 100% certain that a particular Bell state was input. In this USD analysis, we had the BSM circuit announce a determination for an input Bell state only for those detected number states which occur uniquely in the output state for exactly one Bell state, whether for a single value of  $r$  or for all  $r$ . This limited us to the regime where our probability of erroneous state identification ( $p_e$ ) is 0. Here we will expand our performance evaluation to include number states which occur in multiple Bell states, allowing  $p_e > 0$  to produce a higher success probability ( $p_s$ ). Certain applications may benefit from operating in this regime, where an outer layer of quantum error correction may correct for some errors, but gain from a higher rate of success.

We call this operational regime PSD, and define the following probabilities:

- (i)  $p_s + p_e$ : probability that the BSM circuit declares a “success” in identifying the input Bell state.
- (ii)  $1 - (p_s + p_e)$ : erasure probability; BSM circuit declares an “I don’t know” outcome.
- (iii)  $\alpha \equiv p_s / (p_s + p_e)$ : measurement confidence; conditioned on the event that the BSM circuit declares a success,  $\alpha$  is the probability that the input Bell state was indeed correctly identified.

$p_s$  and  $p_e$  will be taken to be averaged over the chosen input Bell state (each of the four assumed to occur equally likely)

and over all PNR detection outcomes. We will now analyze the ( $p_s, p_e$ ) tradeoff, obtained by appropriately postprocessing the PNR detector outputs.

When a number state occurs in multiple output states, instead of rejecting that outcome as erasure, we can use the relative probabilities of its occurrence in each Bell state to decide which Bell state to guess as been input. For instance, at  $r = 0.6$  the state  $|2000\rangle$  occurs in  $|\phi_+''(0.6)\rangle$  and  $|\phi_-''(0.6)\rangle$  with net probabilities 0.230% and 6.41%, respectively. Therefore, if we detect a (2,0,0,0) click pattern on the PNR detectors, we can decide with  $\sim 96.5\%$  certainty that the  $|\phi_- \rangle$  Bell state was the BSM circuit’s input. This increases the success probability ( $p_s$ ) of our BSM circuit by 1.54% when compared with USD operation at  $r = 0.6$ , while introducing a 0.0561% chance of an erroneous measurement ( $p_e$ ).

Considering different subsets of these multiply-occurring number states as valid outcomes, as discussed above, will yield different  $p_s/p_e$  ratios. For our analysis we set a maximum allowable  $p_e$  and then include that subset of duplicate number states which provides an optimal  $p_s$  enhancement for that  $p_e$ , while still considering all other duplicate number states as erasure.

The process for calculating  $p_s$  and identifying optimal subsets of duplicate number states for a given  $p_e$  is detailed in Appendix A 4.

Figure 5 plots  $p_s$  vs  $r$  for PSD operation, assuming lossless (unity detection efficiency) PNR detectors with  $n_{\max} = 7$  number resolution, for a range of error probabilities  $p_e$ . Note that the discontinuous jumps and gaps in  $p_s$  in these plots are not a result of numerical imprecision or algorithmic error. Finite number resolution restricts the number states of interest to a finite set, which is then further restricted to a smaller optimal set by limiting  $p_e$  (see Appendix A 4 for details). This set of interest typically exhibits continuous change in  $p_s$  as  $p_e$  and  $r$  change, but at certain values of  $r$  what constitutes the optimal set of number states of interest changes, resulting in discontinuous jumps of  $p_s$ .

PSD operation gives us access to the previously discontinuous  $p_s$  boost at  $r = 0.6585$  (5.719 dB of squeezing) from Ref. [12] discussed earlier, with very small  $p_e$ . This is an encouraging result, indicating that Zaidi’s and van Loock’s work on USD-boosted BSM [12] is experimentally achievable for near-USD operation; i.e., PSD with very small permitted errors. When higher  $p_e$  is allowed, however, our analysis shows that the squeezing amount  $r$  at which the maximum  $p_s$  occurs is closer to that which maximizes  $p_s$  for USD operation over the continuous regime (rather than where the discontinuous maximum occurs). In other words,  $r = 0.6585$  (5.719 dB of squeezing) ceases to be the optimal squeezing as the allowed  $p_e$  is raised.

### C. Measurement confidence

Determining the effectiveness of a quantum error correction code to correct for an error introduced by a PSD BSM in some application, will require us to know the success (respectively, failure) probability conditioned on the BSM circuit declaring a success. We call this conditional success probability the *measurement confidence*:

$$\alpha = \frac{p_s}{p_s + p_e}. \quad (6)$$

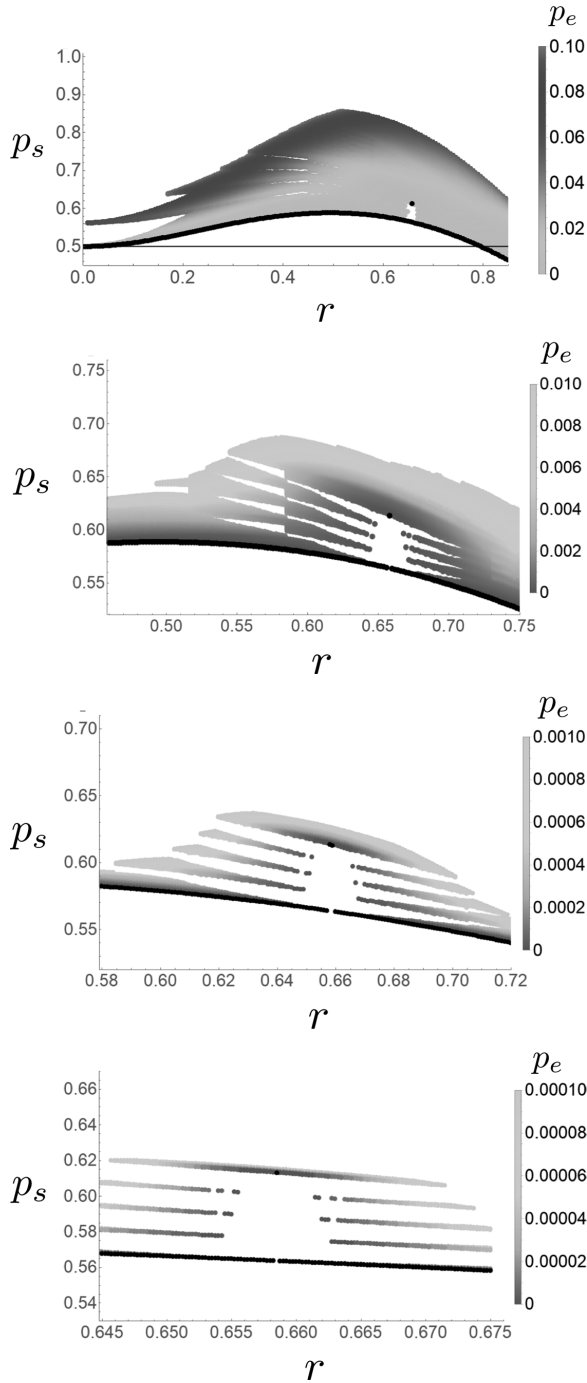


FIG. 5. Bell measurement success probability ( $p_s$ ) vs squeezing amplitude ( $r$ ), with respect to error probability ( $p_e$ ), for a predetection-squeezed BSM circuit, and with PNR detectors restricted to a maximum number resolution  $n_{\max} = 7$ . The black dots represent the results of USD measurements with  $p_e = 0$ . Error probability ( $p_e$ ) is restricted to [0%,10%], [0%,1%], [0%,0.1%], and [0%,0.01%] in the top, second from top, second from bottom, and bottom plots, respectively.

With this in mind we take the data presented in Fig. 5 and neglect  $r$ , instead analyzing  $p_s$  with respect to measurement confidence ( $\alpha$ ), in Fig. 6. Here we see that each value of  $\alpha$  corresponds to a spectrum of points with varied  $p_s$  and  $p_e$ ,

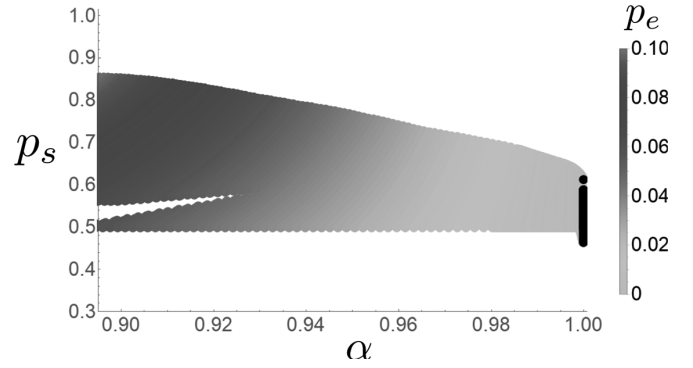


FIG. 6. Bell measurement success probability ( $p_s$ ) vs measurement confidence ( $\alpha$ ), with respect to error probability ( $p_e$ ), for a squeezed Bell measurement circuit, measured with PNR detectors restricted a PNR of  $n_{\max} = 7$ . The black dots represent the results of USD measurements with  $p_e = 0$ .

all with the same ratio  $p_s/(p_s + p_e)$  and therefore equivalent when viewed through the lens of quantum error correction, but with different success probabilities.

From this plot we can obtain a curve showing the maximum success probability obtainable for a given measurement confidence. This curve is plotted in Fig. 7 for a variety of PNR limited detectors, including the current state-of-the-art limit of  $n_{\max} = 7$ . For  $n_{\max} = 7$  we find a maximum  $p_s$  of 85.8% with  $\alpha = 0.889$ , which is produced by  $r = 0.500$  (4.343 dB of squeezing). For  $n_{\max} = \infty$  we find a maximum  $p_s$  of  $\sim 89.5\%$  with  $\alpha \approx 0.90$ , which is produced by  $r = 0.500$  (4.343 dB of squeezing).

#### IV. DETECTOR LOSS

Detector loss is an important impediment in any realistic optical system, especially in quantum information processing applications. Detector losses can be modeled as beam splitters with transmission  $\eta$  prior to an ideal detection, where the reflected photons in the beam splitters are “lost,” and hence cannot be used to discriminate between number states. The process of calculating  $p_s$  for the BSM circuit with lossy detectors, shown in Fig. 8, is detailed in Appendix A 5.

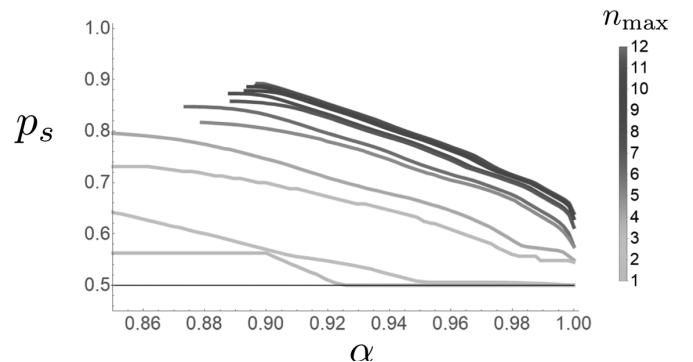


FIG. 7. Maximum Bell measurement success probability ( $p_s$ ) vs measurement confidence ( $\alpha$ ) for a squeezed Bell measurement circuit, shown for PNR detectors with PNR limited to  $n_{\max} \in [1, 12]$ . Each curve terminates at the maximum possible PSD  $p_s$  which can be obtained for a given  $n_{\max}$ .

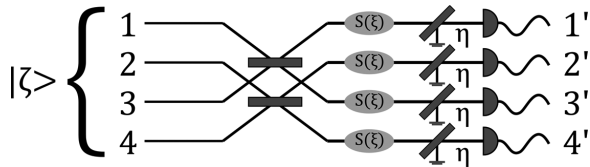


FIG. 8. Predetection quadrature squeezing Bell measurement setup with detector loss represented as predetection beam splitters.

We assume the splitting ratios of all the beam splitters in the BSM circuit to be ideal (i.e., exactly 50-50), and furthermore assume all beam splitters to be lossless (i.e., total input photon number equals the total output photon number). This is because modern beam splitters can be engineered to have extremely low losses, and also because any losses in the beam splitters themselves can be subsumed into detector losses for the purposes of performance evaluation.

The  $n_{\max} = 7$  TES detectors previously cited were experimentally determined to have system device efficiencies ( $\eta$ ) between 98% and 100%, which includes fiber coupling losses [18]. With this value in mind, we evaluated the maximum success probability ( $p_s$ ) obtainable for a given measurement confidence ( $\alpha$ ), as in Fig. 7, for  $\eta \in [0.9, 1]$  with PNR of  $n_{\max} \in [1, 9]$ , shown in Fig. 9. For example, PNR detectors with  $n_{\max} = 7$  and  $\eta = 0.98$  yield a maximum  $p_s$  of 83.3% with  $\alpha = 0.858$ , which is achieved at  $r = 0.480$  (4.169 dB of squeezing).

A full lossy analysis of squeezing-boosted BSMs with PNR  $n_{\max} \geq 10$  could not be performed due to computational limitations.

## V. DISCUSSION AND CONCLUSION

Injection of ancillary single photons or predetection quadrature squeezing can *boost* the success probability  $p_s$  of linear-optical BSM to above the 50% limit. The ability to achieve  $p_s > 0.5$  has been found to be critical in resource-efficient realizations of linear-optical quantum computing and all-photon quantum repeaters [9]. Yet, neither of the aforesaid values of  $p_s > 0.5$  are known to be the maximum achievable using single-photon ancillae and/or squeezing, thereby leaving it open whether  $p_s \rightarrow 1$  might be achievable using these resources. An affirmative conclusion of this open question will not surprise us, given squeezing, linear optics, and PNR detection are in principle universal resources in quantum optics [17].

We reanalyzed previous research predicting a maximum success probability,  $p_s \approx 64.3\%$  for USD-based BSM on linear-optical qubits, employing predetection quadrature squeezing [12]. We showed that the above is a point result, and impossible to achieve experimentally since a small variation in the squeezing amplitude  $r$  drops the USD success probability to about 59%. We showed that, rather unexpectedly, across a large range of squeezing, boosting the BSM success probability above the linear-optic limit of 50% is possible while maintaining USD operation, but that this (experimentally achievable) maximum success rate is significantly lower, 59.6%, achievable with  $r = 0.5774$  ( $\sim 5$  dB of squeezing).

We then considered a PSD framework where we sacrifice pure USD operation, by allowing for a probability of error  $p_e$  conditioned on a “success” being declared (which happens with probability  $p_s + p_e$ ). We find that with a small allowed  $p_e$

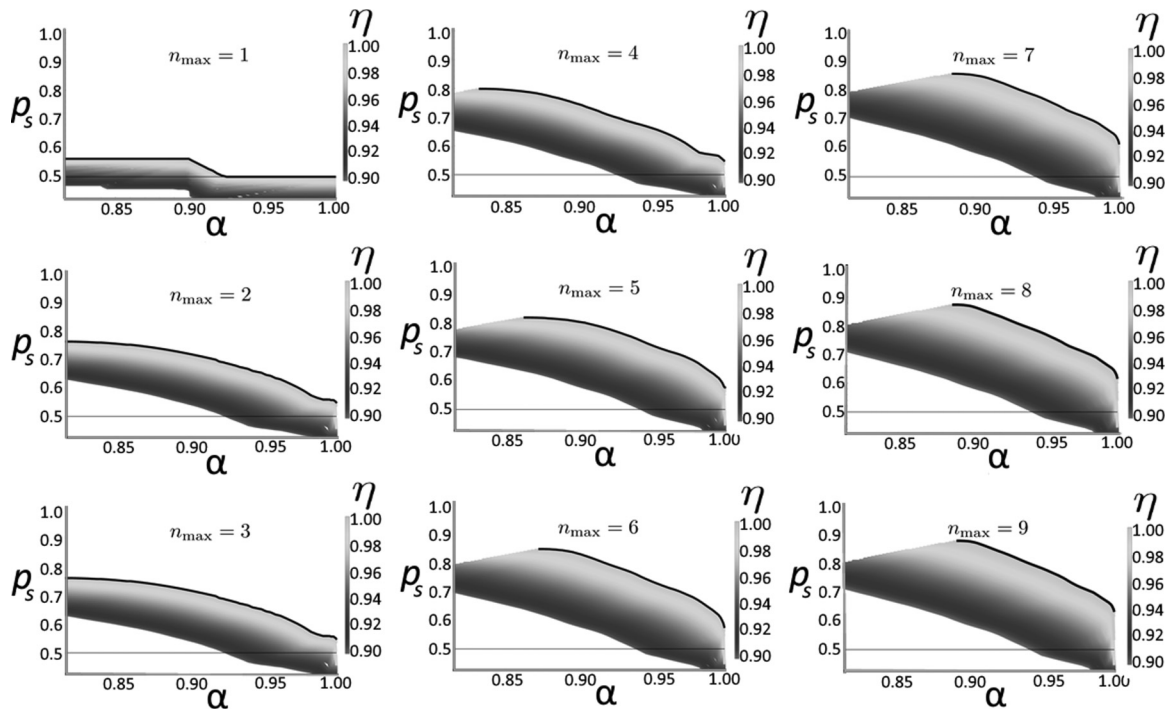


FIG. 9. Maximum Bell measurement success probability ( $p_s$ ) vs measurement confidence ( $\alpha$ ) for a squeezed Bell measurement circuit, shown for lossy PNR detectors with PNR limited to  $n_{\max} = [1, 9]$  with efficiency  $\eta \in [0.90, 1]$ . The black lines represent the success probabilities for lossless detectors shown in Fig. 7.

the 64.3% success probability result of Ref. [12] is achievable over a substantial range of  $r$ .

For PSD measurements, we defined *measurement confidence*  $\alpha = p_s/(p_s + p_e)$  as the probability of correct decision conditioned on a “success” being declared. We found that PSD operation with significantly high error rates (e.g.,  $p_e \sim 0.1$ ) can achieve success rates as high as 89.5% with a measurement confidence of  $\alpha \approx 0.89$ , using  $\sim 5$  dB of predetection squeezing, and PNR detectors with seven-photon resolution. With photon-number resolution and detector inefficiencies possible with the current state-of-the-art TES detectors [18], the maximum achievable success rate,  $p_s \approx 83.3\%$  with a measurement confidence,  $\alpha \approx 0.858$ .

It has recently been shown that arbitrarily large cluster states for all-photonic universal quantum computation can be produced with a supply of three-photon Greenberger-Horne-Zeilinger (GHZ) states, and a Bell state measurement device with success probability  $p_s$  exceeding a threshold of  $\approx 0.59$  (with USD operation). This used ideas from percolation theory [9]. Detector losses within the usual BSM circuits are considered heralded losses since they can be subsumed within  $p_s$ , and maintain USD operation. A complete analysis of percolation-based direct generation of universal photonic cluster states with unheralded losses (e.g., photon losses *after* the creation of the cluster) has not yet been done, leaving open an important question of whether fault-tolerant cluster state quantum computing with ballistic cluster creation is possible with probabilistic boosted BSMs *and* unheralded photon losses. Fault-tolerant universal cluster model quantum computing is known to be possible with single-qubit measurements with conditional probabilities of error below 0.75% (i.e., measurement confidence above 0.9925), where the error model includes preparation, gate, storage, and measurement errors [21].

Our PSD analysis of boosted BSMs can form a starting point of an analysis to see if there is an operational point in the  $p_s$ -vs- $p_e$  trade space where both the percolation condition for long-range connectivity on a subgraph of the Rausendorf-Harrington lattice *and* the error threshold for single-qubit measurements for fault-tolerant operation are satisfied simultaneously. We leave this open for future work. The gate errors in the Rausendorf-Harrington construction for fault-tolerant cluster state quantum computing does not quite translate to BSM error rates (the latter translates to a control-phase two-qubit measurement). However, just to serve as an illustration, in Fig. 10 we show the maximum success probabilities obtainable within a measurement confidence of 0.9925 and above. From this figure it appears that squeezing-boosted BSM devices and PNR detectors with  $n_{\max} \geq 7$  might suffice to realize all-photonic universal quantum computation, with three-photon GHZ states as the initial resource.

Similarly, we believe that our PSD analysis of boosted BSMs can form a starting point of an analysis of a rate-vs-distance calculation for quantum repeaters based on entanglement sources, mode multiplexing, and BSMs [22]. The objective of such an analysis would be to see if there is an optimal operational point in the  $p_s$ -vs- $p_e$  trade space where the rate-vs-loss exponent is minimized, leading to the best possible entanglement generation rate at a given distance,

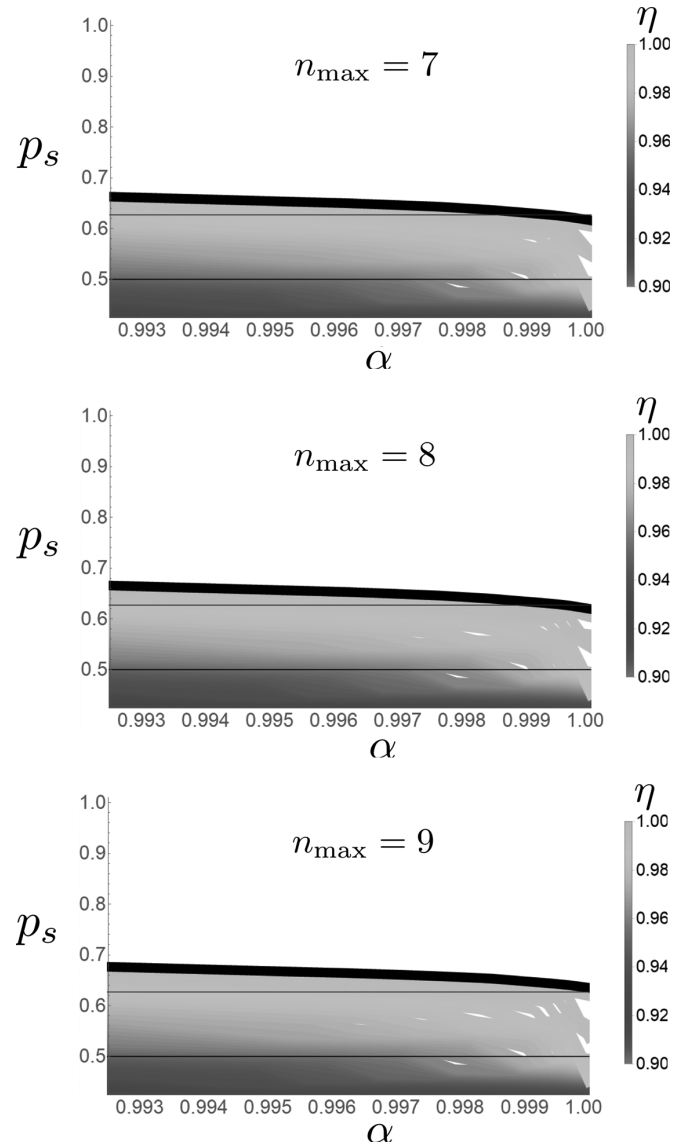


FIG. 10. Maximum Bell measurement success probability ( $p_s$ ) vs measurement confidence ( $\alpha$ ) for a squeezed Bell measurement circuit, shown for lossy PNR detectors with PNR limited to  $n_{\max} = [7, 9]$  with efficiency  $\eta \in [0.90, 1]$ .

when in-line squeezing is used within the BSMs. We leave this for future work as well.

#### ACKNOWLEDGMENTS

This research was funded by an NSF subaward of a Yale University led project, Grant No. 1640959, “EFRI ACQUIRE: Integrated nanophotonic solid state memories for telecom wavelength quantum repeaters.”

#### APPENDIX A: NUMERICALLY COMPUTING BELL MEASUREMENT SUCCESS PROBABILITIES

##### 1. State construction

The first step in evaluating the success probability of a Bell measurement system is constructing the modified Bell states



TABLE I. List of scaled number states from the system detailed in Sec. III, Fig. 2.

$\frac{1}{2} \psi'_+(r)\rangle$	$\frac{1}{2} \psi'_-(r)\rangle$	$\frac{1}{2} \phi'_+(r)\rangle$	$\frac{1}{2} \phi'_-(r)\rangle$
$\frac{i(\operatorname{sech} r)^4}{2\sqrt{2}} 1100\rangle$	$\frac{(\operatorname{sech} r)^4}{2\sqrt{2}} 0110\rangle$	$-\frac{i}{\sqrt{2}}(\operatorname{sech} r)^2 \tanh r 0000\rangle$	$\frac{i(\operatorname{sech} r)^4}{4} 2000\rangle$
$\frac{i(\operatorname{sech} r)^4}{2\sqrt{2}} 0011\rangle$	$-\frac{(\operatorname{sech} r)^4}{2\sqrt{2}} 1001\rangle$	$-\frac{i(\operatorname{sech} r)^4(\cosh 2r-2)}{4} 2000\rangle$	$-\frac{i(\operatorname{sech} r)^4}{4} 0200\rangle$
$\frac{i(\operatorname{sech} r)^4 \tanh r}{4} 0211\rangle$	$\frac{(\operatorname{sech} r)^4 \tanh r}{4} 0112\rangle$	$-\frac{i(\operatorname{sech} r)^4(\cosh 2r-2)}{4} 0200\rangle$	$\frac{i(\operatorname{sech} r)^4}{4} 0020\rangle$
$\frac{i(\operatorname{sech} r)^4 \tanh r}{4} 2011\rangle$	$\frac{(\operatorname{sech} r)^4 \tanh r}{4} 2110\rangle$	$-\frac{i(\operatorname{sech} r)^4(\cosh 2r-2)}{4} 0020\rangle$	$-\frac{i(\operatorname{sech} r)^4}{4} 0002\rangle$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

the system outputs onto its detectors. To do so, we used a simple replacement algorithm for creation operators, derived from (2), where the action of a beam splitter on modes  $j$  and  $k$  is performed as shown in Eqs. (A1).

$$a_j^\dagger \rightarrow \frac{1}{\sqrt{2}}(ia_j^\dagger + a_k^\dagger), \quad (\text{A1a})$$

$$a_k^\dagger \rightarrow \frac{1}{\sqrt{2}}(a_j^\dagger + ia_k^\dagger). \quad (\text{A1b})$$

For a system which involves quadrature squeezing, this replacement algorithm is complicated by the infinite quantity of number states produced by a squeezing operation. When numerically constructing a squeezed state we must use a truncated version of the squeezing operation (4) which does not make use of an infinite series. We show such a truncated squeezing operation below in Eqs. (A2), where the infinite series is truncated by the maximum number state  $|k_{\max}\rangle$ .

$$S(\xi)(a_i^\dagger)^n \rightarrow \left(\frac{1}{\cosh 2r}\right)^{n+1/2} n! \sum_{j=0}^{[n/2]} \frac{(-\xi^*)^j (\cosh 2r)^{2j}}{(n-2j)! j!} \times \sum_{k=0}^{k_{\max}} \frac{\xi^k}{k!} (a_i^\dagger)^{n-2j+2k}, \quad (\text{A2a})$$

$$\xi \equiv \frac{1}{2}e^{i\phi} \tanh r, \quad (\text{A2b})$$

$$\text{dB} = -10 \log_{10}(e^{-2r}). \quad (\text{A2c})$$

Systems with finite PNR  $n_{\max}$  can be exactly evaluated, as truncation is already implied by their finite PNR detectors. Setting  $k_{\max} = \frac{1}{2}(n_{\max} - n + 2j)$  ensures that all of the states

within the detection threshold, and only those states, will be evaluated. (Note that  $j$  is the summation index of the outer sum within which  $\sum_k$  is contained).

To approximate arbitrary photon-number discrimination we set  $n_{\max}$  such that the probability sum of each modified Bell state exceeds 0.999 for  $r \leq 0.70$  and 0.995 for  $0.70 < r \leq 0.90$ . This threshold can be achieved by  $n_{\max} = 13$ . In our calculations  $n_{\max} = 13$  is used to model  $n_{\max} = \infty$ .

(Note that as  $r$  increases more probability gets shifted into larger number states, requiring a higher value of  $n_{\max}$  to fully capture the effects of squeezing).

With this we can produce a finite list of number states and their amplitudes for each modified Bell state, as shown in Table I, where each Bell state is scaled by the square root of its relative probability. (For an equal distribution of Bell states, each state has a  $\frac{1}{4}$  probability of occurrence).

## 2. Separating number states

Now that we have a finite list of number states for each modified Bell state, the next step is to arrange the number states by multiplicity with which they occur in parent Bell states, as shown in Table II. Number states which occur in only one Bell state go to a unique number states list. Number states which occur in multiple Bell states go to a duplicate number states list. (Note: this is the most computationally intensive step of computing Bell measurement efficiencies.)

## 3. USD measurements

To find the USD success probability of a Bell measurement system all one has to do is sum together the modulus squares of all the coefficient terms in the unique number states list.

TABLE II. List of scaled number states from the system detailed in Sec. III, Fig. 2, separated by uniqueness.

Unique number states list $ n_1, n_2, n_3, n_4\rangle_\xi$	Duplicate number states list $ n_1, n_2, n_3, n_4\rangle_\xi$
$-\frac{i}{\sqrt{2}}(\operatorname{sech} r)^2 \tanh r 0000\rangle_{\phi_+}$	$-\frac{i(\operatorname{sech} r)^4(\cosh 2r-2)}{2} 2000\rangle_{\phi_+}, \frac{i(\operatorname{sech} r)^4}{4} 2000\rangle_{\phi_-}$
$\frac{i(\operatorname{sech} r)^4}{2\sqrt{2}} 1100\rangle_{\psi_+}$	$-\frac{i(\operatorname{sech} r)^4(\cosh 2r-2)}{2} 0200\rangle_{\phi_+}, \frac{i(\operatorname{sech} r)^4}{4} 0200\rangle_{\phi_-}$
$\frac{(\operatorname{sech} r)^4}{2\sqrt{2}} 0110\rangle_{\psi_-}$	$-\frac{i(\operatorname{sech} r)^4(\cosh 2r-2)}{2} 0020\rangle_{\phi_+}, \frac{i(\operatorname{sech} r)^4}{4} 0020\rangle_{\phi_-}$
$-\frac{(\operatorname{sech} r)^4}{2\sqrt{2}} 1001\rangle_{\psi_-}$	$-\frac{i(\operatorname{sech} r)^4(\cosh 2r-2)}{2} 0002\rangle_{\phi_+}, -\frac{i(\operatorname{sech} r)^4}{4} 0002\rangle_{\phi_-}$
$\vdots$	$\vdots$

#### 4. PSD measurements

To begin an analysis of PSD success probability we must first note two things. First, not all duplicate number states can provide a boost in Bell state discrimination. Number states which have equal probability in all their parent Bell states have no marginal distinguishability and must be excluded from our analysis. Second, determination of which Bell state is the most probable parent state for a given number state can vary with changes to system parameters. Therefore, any state selection rule applied to number states must be applied on a case by case basis for all parameter values being examined.

To identify an optimal family of duplicate number states for a given error probability and for a given set of parameters we first numerically evaluate the duplicate number state amplitudes corresponding to each Bell state for the given parameters. We then transform the scaled duplicate number state amplitudes to probabilities. Next we identify the total probability for each duplicate number state, over all parent Bell states, and the largest probability provided by an individual Bell state. These two values can be used to compute the expected  $p_s$  and  $p_e$  increases for making Bell state decisions based on a given duplicate number state.

These success probability and error probability increases are then stored as pairs in a list. We then order the list by the  $p_s$  to  $p_e$  ratios of each number state, greatest to least. Each number state is then evaluated in order according to a simple algorithm. If its  $p_e$  increase plus the  $p_e$  increases of all other number states thus far included is less than the maximum allowable  $p_e$ , the number state is included and its efficiency added to the system's total efficiency. If not, it is excluded. All duplicate number states are evaluated in this manner.

(Note that this algorithm only provides an approximately optimal family of duplicate number states under the condition that there exists a very large number of duplicate number states with small  $p_e$  and few if any duplicate number states have high  $p_e$ . This condition is satisfied for all systems analyzed in this paper, but cannot be guaranteed for all systems in general).

#### 5. Lossy measurements

Lossy states are constructed exactly as above in Appendix A 1, using (A3) as the replacement algorithm to model loss.

$$a_i^\dagger \rightarrow \sqrt{\eta} a_i^\dagger + \sqrt{1-\eta} l_i^\dagger. \quad (\text{A3})$$

However, it must be noted that the introduction of loss means that setting  $k_{\max} = \frac{1}{2}(n_{\max} - n + 2j)$  no longer ensures

all states within the detection threshold are evaluated. Doing so excludes larger number states  $\exists i$  s.t.  $n_i > k_{\max}$  which due to loss are detected as number states within the detection threshold  $\forall i, n_i \leq k_{\max}$ . We compensate for this by setting  $n_{\max}$  two higher than its actual value during the state construction algorithm, including the application of loss, and then deleting all creation operators with powers greater than  $n_{\max}$  before evaluating probabilities.

Additionally, each Bell state may now have multiple number states which can be detected as the same photon-number pattern; for instance,  $|1001\rangle$  and  $l_2^\dagger l_3^\dagger |1001\rangle$  are both detected as  $N_1 N_2 N_3 N_4 = 1001$ . Probabilities for photon-number patterns are found by summing the modulus squares of all number states with identical detector patterns within a modified Bell state.

#### APPENDIX B: NONUNIFORM AND PHASE-SHIFTED SQUEEZING

Any numerical analysis of nonuniform quadrature squeezing on Bell measurement systems, where it is not true that  $r_1 = r_2 = r_3 = r_4$ , is complicated by the exponential order of such calculations. With four separately squeezed modes, a coarse scan over squeezing intensity  $r_i \in [0, 0.85]$  with 20 values for each  $r_i$  requires over 100 000 simulation data. This is beyond the scope of the computational capabilities our research group has at its disposal, and we therefore cannot draw any firm conclusions about the potential effects of asymmetric mode squeezing.

However, we did perform a very coarse scan of  $r_i \in \{0, 0.15, 0.30, 0.45, 0.60, 0.6585, 0.75\} \forall i$ , with  $\theta_i = 0 \forall i$ . For the 2401 such points analyzed, there existed no datum with nonuniform squeezing parameters which outperformed all uniformly squeezed data with a shared squeezing parameter. With this in mind we concluded that it is unlikely for nonuniform squeezing intensities to produce improvements over uniform squeezing intensities, but we cannot provide conclusive numerical evidence to back up this assertion.

Nonuniform squeezing phases present an even more computationally intractable problem. Performing enough computations to make even vague assumptions about nonuniform squeezing phases proved too difficult to attempt, and we restricted ourselves to  $\theta_i = 0 \forall i$  to keep the computational complexity of the problem manageable. We have no particular reason to believe  $\theta_i = 0 \forall i$  is optimal. Exploring nonuniform squeezing phases may provide improvements over our results and could be a fruitful area of research for a research group looking to analyze similar systems, particularly with analytic approaches which may be less limited by the computationally intractable nature of the problem.

- 
- [1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).  
 [2] D. Gottesman and I. L. Chuang, *Nature (London)* **402**, 390 (1999).  
 [3] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, *Phys. Rev. Lett.* **71**, 4287 (1993).

- [4] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, *Phys. Rev. Lett.* **76**, 4656 (1996).  
 [5] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, *Nature (London)* **414**, 413 (2001).  
 [6] C. H. Bennett and S. J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).

- [7] E. Knill, R. Laflamme, and G. J. Milburn, *Nature (London)* **409**, (2001).
- [8] J. Calsamiglia and N. Lütkenhaus, *Appl. Phys. B* **72**, 67 (2001).
- [9] M. Pant, D. Towsley, D. Englund, and S. Guha, [arXiv:1701.03775](https://arxiv.org/abs/1701.03775).
- [10] K. Azuma, K. Tamaki, and H.-K. Lo, *Nat. Commun.* **6**, 6787 (2015).
- [11] M. Pant, H. Krovi, D. Englund, and S. Guha, *Phys. Rev. A* **95**, 012304 (2017).
- [12] H. A. Zaidi and P. van Loock, *Phys. Rev. Lett.* **110**, 260501 (2013).
- [13] F. Ewert and P. van Loock, *Phys. Rev. Lett.* **113**, 140403 (2014).
- [14] W. P. Grice, *Phys. Rev. A* **84**, 042331 (2011).
- [15] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, *Phys. Rev. Lett.* **73**, 58 (1994).
- [16] S. L. Braunstein, *Phys. Rev. A* **71**, 055801 (2005).
- [17] S. Lloyd and S. L. Braunstein, *Phys. Rev. Lett.* **82**, 1784 (1999).
- [18] A. E. Lita, B. Calkins, L. A. Pellouchoud, A. J. Miller, and S. Nam, *Proc. SPIE* **7681**, 76810D (2010).
- [19] M. M. Nieto, *Phys. Lett. A* **229**, 135 (1997).
- [20] X.-C. Han, D.-W. Zhuang, Y.-X. Li, J.-F. Song, and Y.-S. Zhang, *Chinese Phys. B* **27**, 074208 (2018).
- [21] R. Raussendorf and J. Harrington, *Phys. Rev. Lett.* **98**, 190504 (2007).
- [22] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, *Phys. Rev. A* **92**, 022357 (2015).