Linear Optics and Projective Measurements for Fun and Profit

Pieter Kok, Hwang Lee, Colin P. Williams, and Jonathan P. Dowling

Quantum Computing Technologies Group, Exploration Systems Autonomy, Section 367
Jet Propulsion Laboratory, MS 126-347
California Institute of Technology
4800 Oak Grove Drive, Pasadena, CA 91109-8099

ABSTRACT

The technique of projective measurements in linear optics can provide apparent, efficient nonlinear interaction between photons, which is technically problematic otherwise. We present an application of such a technique to prepare large photon-number path entanglement. Large photon-number path entanglement is an important resource for Heisenberg-limited optical interferometry, where the sensitivity of phase measurements can be improved beyond the usual shot-noise limit. A similar technique can also be applied to signal the presence of a single photon without destroying it. We further show how to build a quantum repeater for long-distance quantum communication.

Keywords: Linear optical quantum computation, path-entangled state of light, Heisenberg-limited interferometry, single-photon QND measurement, quantum repeater

1. INTRODUCTION

Quantum mechanics enables exponentially more efficient algorithms than can be performed on a classical computer. This discovery has led to the explosive growth of the field of quantum computation.[1] Many physical systems have been suggested for building a quantum computer. These include ion traps, cavity QED, optical systems, quantum dots, nuclear magnetic resonance, and superconducting circuits. Building a quantum computer is a greatest challenge for a future quantum technology, requiring the ability to manipulate quantum-entangled states for millions of sub-components. The concept of a quantum computer is, essentially, the exploitation of quantum interference in obtaining the outcome of a computation. Putting it simply, a quantum computer is a complicated quantum interferometer, and a quantum interferometer is, therefore, a simple quantum computer.

Looking back, quantum computation by linear optics was considered to be doomed by lack of efficient two-qubit logic gates, despite the ease of manipulation of one-qubit gates. Two-qubit gates then necessarily need a nonlinear interaction between the two photons, and the efficiency of this nonlinear interaction is typically very tiny. However, Knill, Laflamme, and Milburn recently showed that this barrier can be circumvented with effective nonlinearities produced by projective measurements,[2] and linear optical quantum computation (LOQC) becomes hopeful. It is fair to say that quantum computers capable of factoring large numbers is still a long shot. But the techniques developed on the road to this holy grail may find useful applications in other technologies such as quantum metrology and communication, which will, in turn, provide the hardware of quantum computing and networking.[3]

We present our recent efforts in quantum state preparation and control by utilizing linear optics and projective measurement and their applications to metrology and communication.

SPIE Conference, Fluctuations and Noise 2003: Noise and Information in Nanoelectronics, Sensors, and Standards (June 1-4, 2003).

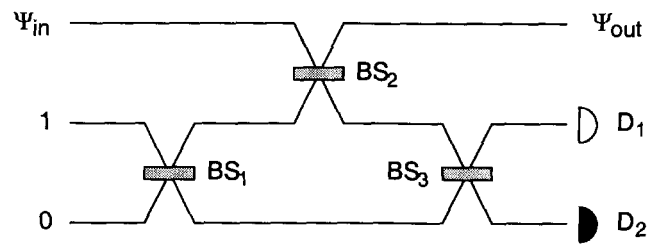

Figure 1. A diagram for nonlinear sign gate. Conditioned upon a specific detector outcome, the desired output state can be obtained by choosing appropriate transmission coefficients of the beam splitters. The success probability of the gate operation is 1/4. But, the merit is that we know it was successful whenever it was successful.

2. EFFECTIVE NONLINEARITIES BY PROJECTIVE MEASUREMENT

Let us consider the Kerr nonlinearity, which can be described by a Hamiltonian[4]

$$\mathcal{H}_{\text{Kerr}} = \hbar\kappa\hat{a}^\dagger\hat{a}\hat{b}^\dagger\hat{b}, \tag{1}$$

where κ is a coupling constant depending on third-order nonlinear susceptibility, and $\hat{a}^\dagger$, $\hat{b}^\dagger$ and $\hat{a}$, $\hat{b}$ are the creation and annihilation operators for two optical modes. One convenient choice of the logical qubit can be then the two modes with a single photon, denoted as

$$\begin{aligned} |0\rangle_L &= |0\rangle_l\,|1\rangle_k \\ |1\rangle_L &= |1\rangle_l\,|0\rangle_k, \end{aligned} \tag{2}$$

where l, k represent the relevant modes, and we have used the notation $|\,\rangle_L$ for logical qubit, in order to distinguish it from the photon-number states.

For a two-qubit gate, let us assign mode 1,2 for the control qubit, and 3,4 for the target qubit. Suppose now only the modes 2,4 are coupled under the interaction given by Eq.(1). For a given interaction time τ, the transformation can be written as

$$\begin{aligned} |0\rangle_L|0\rangle_L &\rightarrow |0\rangle_L|0\rangle_L \\ |0\rangle_L|1\rangle_L &\rightarrow |0\rangle_L|1\rangle_L \\ |1\rangle_L|0\rangle_L &\rightarrow |1\rangle_L|0\rangle_L \\ |1\rangle_L|1\rangle_L &\rightarrow e^{i\varphi}|1\rangle_L|1\rangle_L, \end{aligned} \tag{3}$$

where $\varphi \equiv \kappa n_a n_b \tau$ and $n_a = \langle\hat{a}^\dagger\hat{a}\rangle, n_b = \langle\hat{b}^\dagger\hat{b}\rangle$. This operation yields a conditional phase shift.[5] When $\varphi = \pi$, we have the two two-qubit gate called conditional sign flip gate. A typical two-qubit gate, CNOT, is then simply constructed by using the conditional sign flip and two one-qubit gates (e.g., Hadamard on the target, followed by the conditional sign flip and another Hadamard on the target). In order to have $\varphi \sim \pi$ at the single-photon level, however, a huge third-order nonlinear coupling is required.[6] In stead, Knill, Laflamme, and Milburn devised a nondeterministic conditional sign flip gate using nonlinear sign gate defined by

$$\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \;\longrightarrow\; \alpha|0\rangle + \beta|1\rangle - \gamma|2\rangle. \tag{4}$$

The nonlinear sign gate can be implemented non-deterministically by three beam splitters, two photo-detectors, and one ancilla photon[7] (see Fig. 1). The implementation of conditional sign flip gate is then made by the combination of the nonlinear sign gate and the physics of Hong-Ou-Mandel (HOM) interferometer.[8] For arbitrary two qubits

$$\begin{aligned} |Q_1\rangle &= \alpha_0|0\rangle_L + \alpha_1|1\rangle_L = \alpha_0|0\rangle_1|1\rangle_2 + \alpha_1|1\rangle_1|0\rangle_2, \\ |Q_2\rangle &= \alpha_0'|0\rangle_L + \alpha_1'|1\rangle_L = \alpha_0'|0\rangle_3|0\rangle_4 + \alpha_1'|1\rangle_3|0\rangle_4, \end{aligned} \tag{5}$$

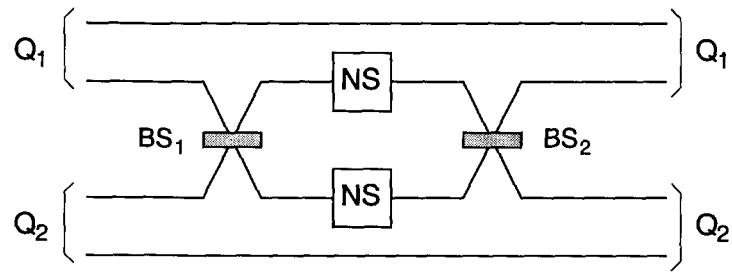

Figure 2. Nondeterministic conditional sign flip gate. The relevant optical modes are assigned as {2,1,3,4} from the top. When the modes 1, and 3 contain one photon each, $|1,1\rangle_{1,3}$ ($|1\rangle_L|1\rangle_L$), it becomes $|2,0\rangle_{1,3} - |0,2\rangle_{1,3}$ after the beam splitter 1. Passing through the nonlinear sign gates, it becomes $-|2,0\rangle_{1,3} + |0,2\rangle_{1,3}$. Beam splitter 2 (conjugate to beam splitter 1) then put this into $-|1,1\rangle_{1,3}$. Obviously, all other input states $|0\rangle_L|1\rangle_L$, $|0\rangle_L|1\rangle_L$, $|1\rangle_L|0\rangle_L$, are not changed.

the transformation by applying a condition sign flip gate, can be written as

$$\begin{aligned} |Q_1\rangle|Q_2\rangle \quad \Rightarrow \quad & \alpha_0\alpha_0'|0\rangle_L|0\rangle_L + \alpha_0\alpha_1'|0\rangle_L|1\rangle_L + \alpha_1\alpha_0'|1\rangle_L|0\rangle_L - \alpha_1\alpha_1'|1\rangle_L|1\rangle_L \\ & = \alpha_0\alpha_0'|0,1,0,1\rangle + \alpha_0\alpha_1'|0,1,1,0\rangle + \alpha_1\alpha_0'|1,0,0,1\rangle - \alpha_1\alpha_1'|1,0,1,0\rangle. \end{aligned} \tag{6}$$

where the modes 1,2 are designated for the control qubit, and 3,4 are for the target qubit. A sign change happens only when there is one photon in mode 1 and one photon in mode 3. The implementation of the desired operation is achieve by two 50/50 beam splitters and two nonlinear sign gates (see Fig. 2), with probability of success 1/16. Effectively, Kerr nonlinearity can be generated by linear optics and projective measurements. The probability of success then can be boosted by using teleportation technique and sufficient number of ancilla photons. It has been also demonstrated that such a nondeterministic two-qubit gate can be made for qubits defined by the polarization degree of freedom,[9,10] which we will discuss in a later section.

3. OPTICAL LITHOGRAPHY BEYOND DIFFRACTION LIMIT

Since the projective measurement can produce an effective photon-photon interaction, it can be a useful tool to manipulate quantum correlation between photons. A particularly interesting type of quantum state of light is the maximally entangled photon-number state. In recent work, it has been shown that the Rayleigh diffraction limit in optical lithography can be overcome[11] by using a quantum state of light of the following form:

$$|\psi\rangle_M = \frac{1}{\sqrt{2}}\left(|N,0\rangle_{ab} + |0,N\rangle_{ab}\right), \tag{7}$$

where a, b denote two different paths. It is well known that the two-photon path-entangled state of Eq. (7) can be generated using a Hong-Ou-Mandel interferometer and two single-photon input states. A 50/50 beam splitter, however, is not sufficient for producing path-entangled states with a photon number larger than two.[12] On the other hand, the generation of these states with $N > 2$ seems to involve a large Kerr nonlinearity, which makes their physical implementation very difficult.[13]

Using the technique of projective measurement, we have shown that by conditioning on single-photon–detection, generation of path-entangled photon-number states is possible for more than two photons.[14] Figure 3 depicts a simple Mach-Zehnder type interferometric scheme for producing such a state with $N = 4$, using dual Fock-state inputs. Suppose that we have the $|3,3\rangle$ state as the input entering into the modes a and b. Then, the first beam splitter transforms $|3,3\rangle$ into a linear superposition of $|6,0\rangle$, $|4,2\rangle$, $|2,4\rangle$, and $|0,6\rangle$. After passing through the two intermediate beam splitters, and if one and only one photon is counted at each detector, the state is then projected onto an equal superposition of $|3,1\rangle$ and $|1,3\rangle$. Simply, the states $|6,0\rangle$ or $|0,6\rangle$ are

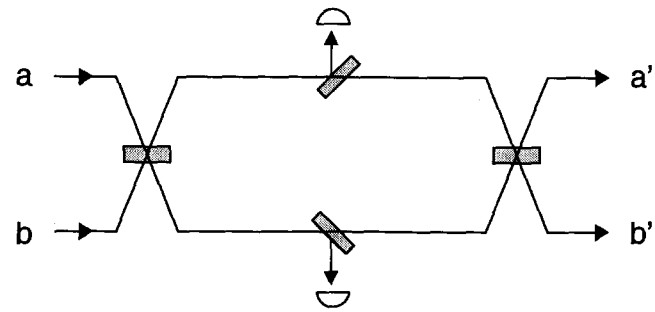

Figure 3. Mach-Zehnder interferometer with two additional beam splitters, which direct the reflected beams to photodetectors. Conditioned on a specific outcome of photodetection, a desired output state can be prepared in the mode a' and b'.

discarded by this feedback from the photodetectors, since they cannot yield a click at both detectors. The $|4,2\rangle$ and $|2,4\rangle$ states, on the other hand, lose one photon in each arm of the interferometer and are projected to $|3,1\rangle$ and $|1,3\rangle$, respectively. Thus, just before the last beam splitter, we have a superposition of $|3,1\rangle$ and $|1,3\rangle$ with a known phase. We use an appropriate phase shifter in one of the two arms of interferometer so that the state after the projective measurement is reduced to $|3,1\rangle - |1,3\rangle$. Consequently after the last beam splitter, we get the desired state $|4,0\rangle - |0,4\rangle$. It has been further shown that it is possible to produce any two-mode, entangled, photon-number state with only linear optical devices conditioned on photodetection.[15] Normally, the probability of success decreases exponentially as N increases.[15–17] For some applications, however, it can be already useful with four-photon entanglement. Quantum interferometric lithography is such an example. It was also proposed in a recent work that the scaling can be sub-exponential in N by using quantum memory.[18] It has been shown that an optimal frequency measurement is achieved by using maximally entangled states of the same form.[19] All the interferometric schemes using entangled or dual-Fock input states show a sensitivity approaching $1/N$ only asymptotically. However, using the maximally entangled states of Eq. (7), the phase sensitivity is equal to $1/N$, even for a small N.

4. PHASE NOISE REDUCTION BEYOND SHOT-NOISE LIMIT

In a typical optical interferometer in which ordinary coherent laser light enters via one input port, the phase sensitivity in the shot-noise limit scales as $\Delta\varphi = 1/\sqrt{\bar{N}}$ where $\bar{N}$ is the mean number of photons. Over the last two decades a lot of effort was devoted to overcome this limit, with obvious practical applications. In the early 1980's, Caves first demonstrated that squeezing the vacuum in the unused input port of the interferometer causes the phase sensitivity to beat the standard shot-noise limit.[20] In 1986, it was shown that phase noise reduction can be achieved using input light with photon-number eigenstates, incident upon both input ports of a Mach-Zehnder interferometer. In particular, Yurke and collaborators showed that if the photons entered into each input port of the interferometer in nearly equal numbers with certain type of correlation, then, it was possible to obtain an asymptotic phase sensitivity of $1/N$, the Heisenberg limit.[21,22] The so-called Yurke state is of the form:

$$|\psi\rangle_{\mathrm{Y}} = \frac{1}{\sqrt{2}}\left[\left|\tfrac{N+1}{2},\tfrac{N-1}{2}\right\rangle_{ab} + \left|\tfrac{N-1}{2},\tfrac{N+1}{2}\right\rangle_{ab}\right], \tag{8}$$

where a, b denote the two input modes. Then, in the early 1990's, Holland and Burnett proposed Heisenberg-limited interferometry by the use of so-called ***dual Fock states*** of the form[23]:

$$|\psi\rangle_{\mathrm{D}} = |N,N\rangle_{ab}. \tag{9}$$

Such a state can be generated, for example, by degenerate parametric down conversion, or by optical parametric oscillation. In a conventional Mach-Zehnder interferometer only the difference of the number of photons at

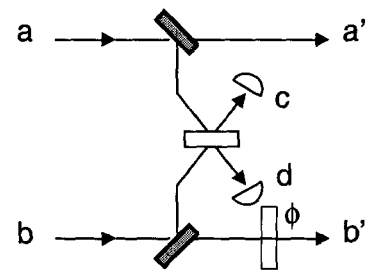

Figure 4. A simple path-entanglement generator. Yurke-type quantum correlation between the two modes can be produced with a dual Fock-state. Suppose we post-select the outcome, conditioned upon only one photon detection by either one of the two detectors. Due to the 50/50 beam splitter in the midway, it is not possible to tell whether mode a or b lost one photon. The fundamental lack of which-path information provides the entanglement between the two output modes. For two-fold coincidence detection, the two detected photons are from either mode a or mode b, which eliminates the possibility of peeling off one photon from each mode.

the output is measured. However, to obtain increased sensitivity with dual Fock states, some special detection scheme is required.[24] A combination of a direct measurement of the variance of the difference current as well as a data-processing method based on Bayesian analysis, was proposed by Kim and collaborators.[25] Berry and Wiseman have proposed an adaptive measurement scheme with an optimal input state.[26]

The Yurke state approach has the same measurement scheme as the conventional Mach-Zehnder interferometer; a direct detection of the difference current. It is, however, not easy to generate the desired correlation in the input state. On the other hand, the dual Fock-state approach finds a rather simple input state, but requires a complicated data processing methods. However, by a simple utilization of the projective measurements with linear optical devices, it is possible to generate a desired correlation in the Yurke state directly from the dual Fock state.[3] A similar method has been proposed for matter-wave interferometers using Bose-Einstein condensates.[27] Consider a linear optical setup depicted in Fig. 4. For a given dual Fock-state input $|N, N\rangle_{ab}$, the output state conditioned on, for example, a two-fold coincident count is given by

$$\frac{1}{\sqrt{2}}\left[|N, N-2\rangle + |N-2, N\rangle\right]. \tag{10}$$

Here the maximum probability success of this event can be optimized by choosing the reflection coefficient $|r|^2 = 1/N$, and its asymptotic value can be found as $1/(2e^2)$, independent of N. Furthermore, using a stack of such devices with appropriate phase shifters, generation of maximally path-entangled states of the form Eq. (7) with an arbitrary number of photons has been developed.[15]

5. SINGLE-PHOTON QND MEASUREMENT DEVICES

In a quantum nondemolition (QND) measurement an observable is measured and the back-action noise is coupled only to the conjugate of the measured quantity. The system is projected to a corresponding eigenstate and repeated QND measurements then yield the same result as the initial measurement. This can provide a sensitive probe of the perturbation causing any difference between results of two consecutive measurements.

In quantum optics QND devices are usually considered in the context of photon-number measurements. Common photodetection is based on destroying photons that they detect. Hence, the basic idea of QND in quantum optics is to couple the signal beam to the 'meter' beam in a nonlinear medium, and the detection of the phase shift of the meter beam measures the number of photons in the signal beam.[28] QND schemes of this type include an optical Kerr medium, a parametric amplifier, and cold atoms in a magneto-optical trap. The readouts of the number of photons in the signal beam are performed by phase-sensitive homodyne detection of the meter beam in interferometer arrangements. In a recent experiment, a single-photon QND has been demonstrated by using a resonant coupling between the cavity field and the meter atoms.[29]

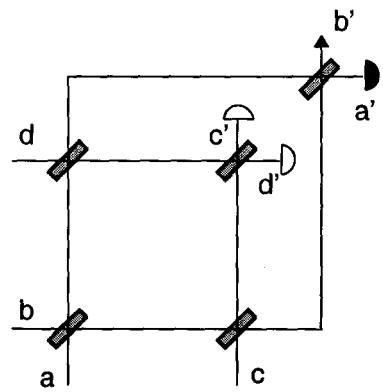

Figure 5. QND measurement device for single-photon detection. The input state, of an arbitrary superposition of $|0\rangle$, $|1\rangle$, and $|2\rangle$, enters into mode a, and an auxiliary single photon is prepared for both modes c and d. Conditioned upon a detector coincidence in modes c' and d', and no count in mode a', the outgoing mode b' is a single-photon state.

Such a QND device at the single photon level can provide a key tool for optical quantum information processing, perhaps most importantly in quantum error correction. However, as we discussed in section 2, the required nonlinearities become too large for single-photon level. Instead, using the technique of projective measurement, we have proposed a probabilistic device that signals the presence of a single photon without destroying it.[30]

A simple way to perform a single-photon QND measurement is to use quantum teleportation. For example, a maximally polarization-entangled photon pair produced by a parametric down-converter can serve as a quantum channel. If the input state is in a arbitrary superposition of zero and one photon with a fixed polarization, the detector coincidence in Bell state measurement, signals the present of a single photon in the input and also the output states. Simply, a vacuum input can never yield a two-fold detector coincidence. This teleportation scheme, however, breaks down in the case where the input state is of the form:

$$|\psi\rangle_{in} = c_0|0\rangle + c_1|1\rangle + c_2|2\rangle. \tag{11}$$

The two-photon term will contribute to the two-fold coincidence even when the output of the down-converter is vacuum, yielding a false identification of a single photon in the output state, conditioned on a detector coincidence.

We can eliminate such a false identification by using an interferometric setup depicted in Fig.5. It is not a full QND measurement of the photon-number observable since it works for only zero, one and two photons. It can, however, still play an important role in linear optical quantum computation, where up to only two photons are used in each logic gate. In Fig. 5, we assume that the input state of the for Eq.(11) enters into in mode a, and further prepare single photons for mode c and d. The transformation of the probe photons in the mode c and d can then be written as

$$\hat{c}^\dagger \hat{d}^\dagger \rightarrow \frac{1}{4}(\hat{b}'^{\dagger 2} - \hat{a}'^{\dagger 2} + \hat{d}'^{\dagger 2} - \hat{c}'^{\dagger 2} - 2\hat{a}'^\dagger \hat{c}'^\dagger + 2\hat{b}'^\dagger \hat{d}'^\dagger). \tag{12}$$

Then we post select photodetection outcome as one and only one photon counted at each detector. This condition requires either two photons in mode c or two photons in mode d, which eliminate the contribution from $c_0|0\rangle$ of the input state. For one-photon and two-photon input states, we have

$$\hat{a}^\dagger \rightarrow \frac{1}{\sqrt{2}}(\hat{a}'^\dagger - \hat{c}'^\dagger) \tag{13}$$

$$\hat{a}^{\dagger 2} \rightarrow \frac{1}{2}(\hat{a}'^{\dagger 2} - 2\hat{a}'^\dagger \hat{c}'^\dagger + \hat{c}'^{\dagger 2}). \tag{14}$$

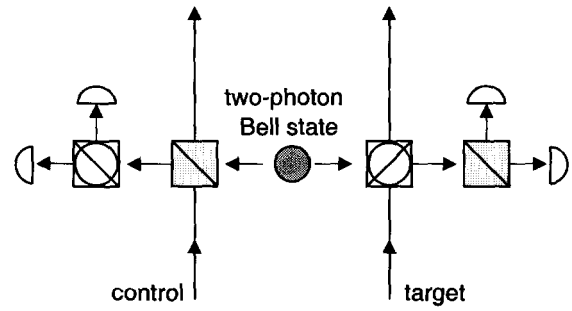

Figure 6. A probabilistic CNOT gate using two polarization beam splitters and $\pi/4$-rotated polarization beam splitters. Conditioned on specific photo-detection outcome, CNOT can be perform with probability 1/4.[10]

Now the only two-fold coincidence in the mode c' and d' by a two-photon input is possible when the $2\hat{b}'^\dagger\hat{d}'^\dagger$ form Eq.(12) and $2\hat{a}'^\dagger\hat{c}'^\dagger$ from Eq.(14), yielding $\hat{a}'^\dagger\hat{b}'^\dagger\hat{c}'^\dagger\hat{d}'^\dagger$. However, further postselecting on vacuum in the mode a' eliminate this two-photon contribution to the two-fold coincidence in c' and d'. Finally, for a single photon in mode a yields a contribution $\hat{b}'^\dagger\hat{c}'^\dagger\hat{d}'^\dagger$, saying that there is a two-fold coincidence in mode c' and d', and a single photon in the output mode b'. As can be seen if Eqs.(12,13), the efficiency of this interferometric device with 50:50 beam splitters is 1/8. By choosing the transmission coefficients of the beam splitters in modes c and d, the probability of success becomes 4/27. Obviously, this scheme does not work down when the incoming state with a unknown polarization. However, it turns out that a more sophisticated interferometric setup with polarization beam splitters can do the job with preserving the unknown polarization.[30]

6. NONDETERMINISTIC CNOT AND QUANTUM REPEATERS

The concept of quantum repeaters has been proposed for single-photon optical quantum communication over distances longer than the attenuation length of the channels used.[31] Quantum repeaters employ a combination of entanglement purification[32] and swapping. Many pairs of degraded entangled states are purified to fewer maximally entangled states, after which swapping is used to extend the, now maximal, entanglement over longer distances.

For entanglement purification, both Alice and Bob apply a CNOT, where the halves of the first entangled state pair serve as the control qubit, and the halves of the second as the target. The target qubits are then measured in the computational basis ($|H\rangle$ and $|V\rangle$), and conditioned on a parallel coincidence ($|H\rangle_A|H\rangle_B$ or $|V\rangle_A|V\rangle_B$), Alice and Bob now share a maximally entangled state in the remaining two qubits. The probability of purification depends on the fidelity of the incoming entangled states, and therefore on the channel noise factor γ. The entanglement swapping component is essentially a Bell detector. It is well known that it is impossible to make a deterministic, complete, Bell measurement with linear optics,[33] but one can distinguish two out of four two-qubit Bell states with a simple beam splitter configuration.[34] Recently, Franson and co-workers have shown that a CNOT (and hence a Bell measurement) is possible nondeterministically with only projective measurements and entangled input states.[10,35] The probability of success for this CNOT is not large enough to make the Bell measurement more efficient, but it will be an essential component of our purifier. Based on linear optics and an entangled-photon source we have developed a protocol for optical quantum repeaters.[36]

The source for polarization-entangled photon pairs has mostly consisted of parametric down-converters, where a strong pump laser is sent through a nonlinear crystal. However, the output of these devices are not clean, maximally entangled, two-photon states, but rather a coherent superposition of multiple pairs. For large-scale applications, one needs many entangled photon pairs, which would require, say, N down-converters to fire in unison. This happens with probability $|\epsilon|^{2N}$, where $|\epsilon|^2$ is the probability of creating a maximally entangled state. However, with approximately the same probability the first down-converter produces N photon pairs, while the others produce nothing. Any distribution of N photon pairs scales proportional to $|\epsilon|^{2N}$. Therefore, an array of N parametric down-converters hardly meets the desired properties as push-button production of a polarization-entangled photon-pair and high fidelity of the output. One entanglement source that very nearly

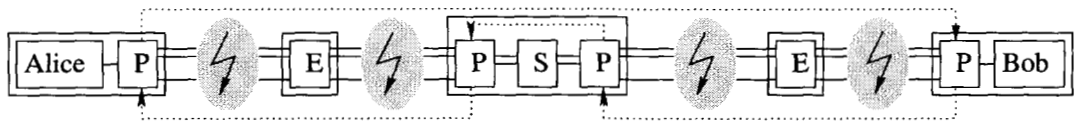

Figure 7. The schematic of a quantum repeater. E, P, and S denote the entangled-photon sources, the purifier and the swapping element, respectively. The solid lines represent quantum channels and the dotted lines are for classical channels.

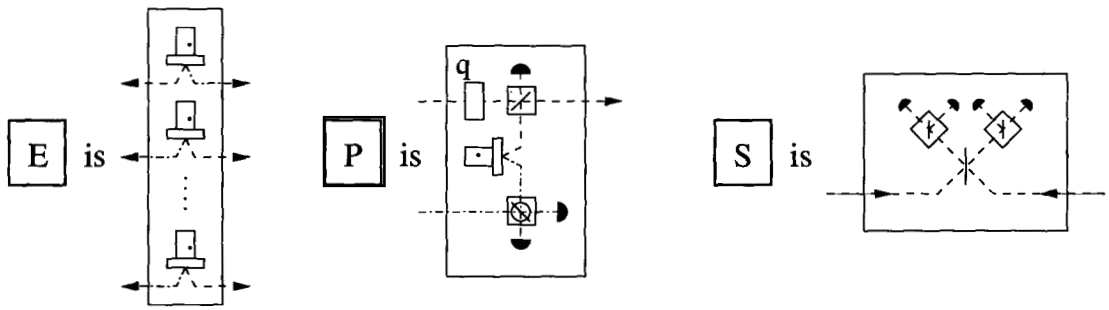

Figure 8. The components of the quantum repeater. The purifier element contains a QND device, an optical CNOT gate, and a detector on one output mode. The swapper implements a partial Bell measurement.[36]

meets our requirements has been proposed by Yamamoto and co-workers[37] using a quantum dot separating p-type and n-type GaAs is sandwiched between two Bragg mirrors. In particular, the probability of creating a pair can be as high as $p_s = 0.9$.

Figure 7 shows the schematic of a quantum repeater, where the shaded region represents the decoherence during transmission. The separate components of a quantum repeater are depicted in Fig. 8. Additionally, we need to check if the modes of the control qubit might be empty, since the entanglement source failed to create a photon. In order to rule out these events, we can employ the single-photon QND measurement device, which signals a single photon in an optical mode without destroying its polarization as discussed in the previous section.

Let us consider the probability of success for the individual components, as well as the losses in the system. For purification, we need two CNOT and a QND device, and at least two double-photon guns. Each CNOT need one double-photon gun and two more guns are needed for the QND. Hence total of six double-photon guns are required. Also, ten photodetectors are needed (three per CNOT and four in the QND device). We assume that all the detectors have the same quantum efficiency η. The noise parameters due to the attenuation are given by γ for the dephasing, and ζ for the photon loss over the channel. The probability for purifying a single pair of entangled photons is then given by

$$p_{\text{pur}} = p_s^6 \, \eta^{10} \, (1-\gamma)^2 \, \zeta^2 \, p_{\text{CNOT}}^2 \, p_{\text{QND}}, \tag{15}$$

where p_s is the probability of success of the double-photon gun. Furthermore, a complete Bell detection occurs only 50% of the time. The probability of success for entanglement swapping is therefore given by

$$p_{\text{swap}} = \frac{\eta^2}{2}. \tag{16}$$

Since a repeater needs two purifiers and one swapper, the total number of components N_{total} is given by $N_{\text{total}} = 2N_{\text{pur}}N_{\text{swap}}$. Let us take typical values of the parameters, for example, $p_s = 0.9$, $\gamma = 0.5$, $\zeta = 1/\sqrt{2}$, $p_{\text{CNOT}} = 1/4$, and $p_{\text{QND}} = 1/8$. Then, for $\eta = 0.3$, we have $N_{\text{total}} \approx 10^9$. Choosing $\eta = 0.8$, we obtain $N_{\text{total}} \approx 10^4$. It is immediately clear that an improvement in the detector efficiency yields a substantial gain in the efficiency of the protocol, due to the factor η^{10} in Eq.(15). Therefore, in order to operate the repeater more efficiently, better detectors are needed.

7. SUMMARY

Linear optics with measurements of some part of the system, i.e., projective measurements, can sometimes replace the use of Kerr nonlinearities, but with much higher efficiency. Using this technique we have studied generation of useful photonic quantum correlations. The maximally path-entangled photon-number states provide an essential way for optical lithography to proceed beyond the Rayleigh diffraction limit. The Yurke-type path-entanglement is of particular importance in Heisenberg-limited interferometry. Projective measurements also enable us to construct a device that signals the presence of a single photon without destroying it. Single-photon non-demolition measurement bears a great importance in optical quantum computing, since most error-correction codes in presence of qubit loss requires QND measurements. Finally, using only LOQC elements and our QND scheme, we showed how to build a quantum repeater that faithfully transmits flying qubits between distant locations. Since all of the devices mentioned here heavily rely on the feedback from the detectors, the quantum efficiency and multi-photon resolution of a photodetector plays the key role in their practical implementation.

ACKNOWLEDGMENTS

This work was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. The authors wish to thank C. Adami, N.J. Cerf, J.D. Franson, G.J. Milburn, W.J. Munro, and T.B. Pittman for helpful discussions. P.K. and H.L. acknowledge the National Research Council. We would like to acknowledge support from the National Security Agency, the Advanced Research and Development Activity, the Defense Advanced Research Projects Agency, the National Reconnaissance Office, and the Office of Naval Research.

REFERENCES

1. J.P. Dowling and G.J. Milburn, "Quantum Technology: The second Revolution," (in press) Phil. Trans. Roy. Soc. (London, 2003), quant-ph/0206091.
2. E. Knill, R. Laflamme, and G.J. Milburn, "A scheme for efficient quantum computation with linear optics," Nature **409**, 46 (2001).
3. H. Lee, P. Kok, and J.P. Dowling, "A quantum Rosetta stone for interferometry," J. Mod. Opt. **49**, 2325 (2002).
4. M.O. Scully and M.S. Zubairy, *Quantum Optics* (Cambridge University Press, Cambridge, UK, 1997).
5. Q.A. Turchette *et al.*, "Measurement of conditional phase shifts for quantum logic," Phys. Rev. Lett. **75**, 4710 (1995).
6. G.J. Milburn, "Quantum Optical Fredkin Gate," Phys. Rev. Lett. **62**, 2124 (1989).
7. T.C. Ralph, A.G. White, W.J. Munro, and G.J. Milburn, "Simple scheme for efficient linear optics quantum gates," Phys. Rev. A **65**, 012314 (2001).
8. C.K. Hong, Z.Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," Phys. Rev. Lett. **59**, 2044 (1987).
9. M. Koashi, T. Yamamoto, and N. Imoto, "Probabilistic manipulation of entangled photons," Phys. Rev. A **63**, 030301(R) (2001).
10. T.B. Pittman, B.C. Jacobs, and J.D. Franson, "Probabilistic quantum logic operations using polarizing beam splitters," Phys. Rev. A **64**, 062311 (2001).
11. A.N. Boto *et al.*, "Quantum interferometric optical lithography: Exploiting entanglement to beat the diffraction limit," Phys. Rev. Lett. **85**, 2733 (2000).
12. R.A. Campos, B.E.A. Saleh, and M.C. Teich, "Quantum-mechanical lossless beam splitter: SU(2) symmetry and photon statistics," Phys. Rev. A **40**, 1371 (1989).
13. C.C. Gerry and R.A. Campos, "Generation of maximally entangled photonic states with a quantum-optical Fredkin gate," Phys. Rev. A **64** 063814 (2001).
14. H. Lee, P. Kok, N.J. Cerf, and J.P. Dowling, "Linear optics and projective measurements alone suffice to create large-photon-number path entanglement," Phys. Rev. A **65**, 030101 (R) (2002).
15. P. Kok, H. Lee, and J.P. Dowling, "The creation of large photon-number path entanglement conditioned on photodetection," Phys. Rev. A **65**, 052104 (2002).

16. J. Fiurásek, "Conditional generation of N-photon entangled state of light," Phys. Rev. A **65**, 053818 (2002).
17. X.B. Zou, K. Pahlke, and W. Mathis, "Generation of entangles photon states by using linear optical elements," Phys. Rev. A **66**, 014102 (2002).
18. N.J. Cerf, J. Fiurasek, S. Iblisdir, and S. Massar, "Generation of large photon-number cat states using linear optics and quantum memory," quant-ph/0210059 (2002).
19. J.J. Bollinger W.M. Itano, and D.J. Wineland, and D.J. Heinzen, "Optimal frequency measurements with maximally correlated states," Phys. Rev. A **54**, R4649 (1996).
20. C.M. Caves, "Quantum mechanical noise in an interferometer," Phys. Rev. D **23**, 1693 (1981).
21. B. Yurke, "Input state for enhancement of fermion interferometer sensitivity," Phys. Rev. Lett. **56**, 1515 (1986).
22. B. Yurke, S.L. McCall, and J.R. Klauder, "SU(2) and SU(1,1) interferometers," Phys. Rev. A **33**, 4033 (1986).
23. M.J. Holland and K. Burnett, "Interferometric detection of optical phase shifts at the Heisenberg limit," Phys. Rev. Lett. **71**, 1355 (1993).
24. B.C. Sanders and G.J. Milburn, "Optimal quantum measurements for phase estimation," Phys. Rev. Lett. **75**, 2944 (1995).
25. T. Kim *et al.*, "Influence of decorrelation on Heisenberg-limited interferometry with quantum correlated photons," Phys. Rev. A **57**, 4004 (1998).
26. D.W. Berry and H.M. Wiseman, "Optimal states and almost optimal adaptive measurements for quantum interferometry," Phys. Rev. Lett. **85**, 5098 (2000).
27. J.P. Dowling, "Correlated input, matter-wave interferometer: Quantum-noise limits to the atom-laser gyroscope," Phys. Rev. A **57**, 4736 (1998).
28. P. Grangier, J.A. Levenson, and J.-P. Poizat, "Quantum non-demolition measurements in optics," Nature **396**, 537 (1998).
29. G. Nogues *et al.*, "Seeing a single photon without destroying it," Nature **400**, 239 (1999).
30. P. Kok, H. Lee, and J.P. Dowling, "Single-photon quantum nondemolition detectors constructed with linear optics and projective measurements," Phys. Rev. A **66**, 063814 (2002).
31. H.-J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," Phys. Rev. Lett. **81**, 5932 (1998).
32. C.H. Bennett *et al.*, "Purification of noisy entanglement and faithful teleportation via noisy channels," Phys. Rev. Lett. **76**, 722 (1996).
33. N. Lütkenhaus, J. Calsamiglia and K.-A. Suominen, "Bell measurements for teleportation," Phys. Rev. A **59**, 3295 (1999).
34. S.L. Braunstein and A. Mann, "Measurement of the Bell operator and quantum teleportation," Phys. Rev. A **51**, R1727 (1995).
35. T.B. Pittman, B.C. Jacobs, and J.D. Franson, "Demonstration of nondeterministic quantum logic operations using linear optical elements," Phys. Rev. Lett. **88**, 257902 (2002).
36. P. Kok, C.P. Williams, and J.P. Dowling, "Practical quantum repeaters with linear optics and double-photon guns," (in press) Phys. Rev. A, quant-ph/0203134 (2002).
37. O. Benson, C. Santori, M. Pelton, and Y. Yamamoto, "Regulated and entangled photons from a single quantum dot," Phys. Rev. Lett. **84**, 2513 (2000).