Probabilistic quantum logic operations using polarizing beam splitters

T. B. Pittman, B. C. Jacobs, and J. D. Franson

Applied Physics Laboratory, The Johns Hopkins University, Laurel, Maryland 20723

It has previously been shown that probabilistic quantum logic operations may be performed using linear optical elements, additional photons (ancilla), and post-selection based on the output of single-photon detectors. Here we describe the operation of several quantum logic operations of an elementary nature, including a quantum parity check and a quantum encoder, and we show how they may be combined to implement a controlled-NOT (CNOT) gate. All of these gates may be constructed using polarizing beam splitters that completely transmit one state of polarization and totally reflect the orthogonal state of polarization, which allows a simple explanation of each operation. We also describe a polarizing beam splitter implementation of a CNOT gate that is closely analogous to the quantum teleportation technique previously suggested by Gottesman and Chuang [Nature **402**, 390 (1999)]. Finally, our approach has the interesting feature that it makes practical use of a quantum-eraser technique.

I. INTRODUCTION

An optical approach to quantum information processing would have several advantages, including the ability to transport qubits from one location to another using optical fibers or waveguides. The main difficulty with any optical approach is that nonlinear interactions between individual photons are required in order to implement quantum logic gates that operate with 100% efficiency. It was recently shown in two pioneering papers [1,2], however, that probabilistic quantum logic gates may be implemented using linear optical elements, additional photons (ancilla), and post selection based on the output of single-photon detectors. Probabilistic logic gates of this kind will give the desired result with certainty when a specific output from the detectors is obtained, but that will only occur for some fraction of the events, typically with a probability of 1/16 to 1/4. Somewhat remarkably, Knill, LaFlamme, and Milburn (KLM) [1] have shown that the probability of success of a given operation can approach unity in the limit of large numbers of ancilla and detectors [3].

In this paper, we describe a variety of quantum logic gates that may be constructed using polarizing beam splitters that completely transmit one state of polarization and totally reflect the orthogonal state of polarization. One advantage of this approach is that it enables us to give simple explanations for the operation of all of the relevant quantum logic gates. In addition, polarization-encoded qubits are typically less sensitive to phase drifts than are interferometric implementations. We describe several kinds of probabilistic quantum logic gates, including a quantum parity check and a quantum encoder, along with two different implementations of the controlled-NOT (CNOT) gate.

The original two approaches [1,2] for implementing probabilistic quantum logic gates using linear elements are closely related to an earlier paper by Gottesman and Chuang (GC) [4], who showed that a CNOT gate could be implemented using a modified form of quantum teleportation [5] and a four-qubit entangled state as a resource (ancilla). The Bell-state measurements [6] required for teleportation are in-

herently nonlinear [7–9], but a partial set of Bell measurements may be performed probabilistically using linear optical elements [10–12]. Combining these two ideas leads to a CNOT gate that we describe in Sec. II using polarizing beam splitters. As we already mentioned, this approach provides a straightforward way to understand the operation of the logic gate as well as some potential experimental advantages in its operation. This CNOT gate is similar in some respects to those previously described by KLM [1] as well as by Koashi, Yamamoto, and Imoto (KYI) [2].

In Sec. III, we introduce several simple quantum logic gates that combine two photons on a single polarizing beam splitter to perform a variety of elementary functions, including a destructive-CNOT gate in addition to the quantum parity check and quantum encoder mentioned above. These elementary operations are then combined to give an alternative implementation of a complete probabilistic CNOT gate that does not rely on teleportation in any obvious way.

Our approach makes use of a technique that may be viewed as being equivalent to a quantum eraser [13–15], as is described in the Appendix. We summarize our results and consider the prospects for future applications in Sec. IV.

II. CNOT GATE USING FOUR-PHOTON ENTANGLED STATES

As we mentioned earlier, Gottesman and Chuang showed in a pioneering paper [4] that a CNOT operation could be performed using a modified form of quantum teleportation. Although the required Bell-state measurements are inherently nonlinear [7–9], a partial or incomplete set of Bell-state measurements may be implemented using linear optical elements and post selection, as has been demonstrated experimentally by Zeilinger's group [10–12]. A combination of these two techniques might be expected to allow the implementation of a probabilistic CNOT, which formed part of the motivation for earlier work in this area [1,2]. Here, we describe an implementation of a probabilistic CNOT along these lines using polarizing beam splitters and a quantum erasure technique. This approach requires ancilla in the form of a
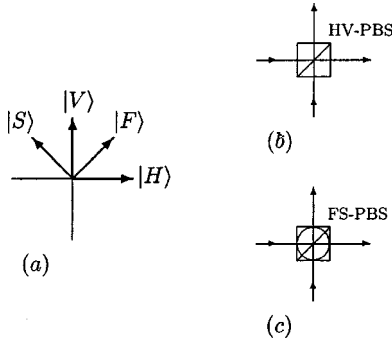
FIG. 1. (a) Orientations of the HV and FS polarization bases used throughout the text. The FS basis is rotated $+45°$ with respect to the HV basis. (b) and (c) show the symbols used to represent polarizing beam splitters in the HV and FS bases, respectively.

four-photon entangled state $|\chi\rangle$ that can be created in various ways [1,2,4], as will be discussed further in Sec. IV below. The implementation given here is similar in spirit to those of Refs. [1] and [2], but our approach allows a more straightforward understanding of the operation of the CNOT gate and may have some practical advantages as well.

The polarization conventions that will be used throughout the paper are shown in Fig. 1. The photonic qubits $|0\rangle$ and $|1\rangle$ will be represented by horizontal $|H\rangle$ and vertical $|V\rangle$ polarizations, respectively, but measurements will also be made in the $|F\rangle$ and $|S\rangle$ basis shown in the figure [16]. Polarizing beam splitters oriented in the HV basis will always transmit H-polarized photons and reflect V-polarized photons, while polarizing beam splitters oriented in the FS basis will transmit F-polarized photons and reflect S-polarized photons. It will be assumed throughout the paper that the beam splitters and detectors are ideal and that all the photons in a given optical path are in the same spatial mode [17–20].

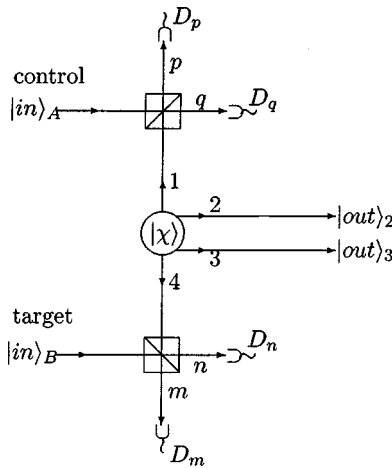Figure 2 shows an implementation of a CNOT gate using

FIG. 2. A polarization-encoded version of the Gottesman-Chuang protocol. This scheme relies on a four-photon entangled state $|\chi\rangle$ to perform a probabilistic CNOT operation on the two input photonic qubits in modes A and B. Four polarization-sensitive detectors in the FS basis are labeled D_m, D_n, D_p, and D_q.

the GC protocol [4] with polarization-encoded photonic qubits and partial Bell-state measurements. At the center of the figure is a source that emits the four-photon entangled state $|\chi\rangle$, whose properties we will now investigate. The state $|\chi\rangle$ is created in such a way that one photon is emitted into each of the four modes labeled 1 through 4.

The input photon in mode A is mixed with the photon in mode 1 by a polarizing beam splitter in the HV basis with ideal single-photon detectors D_p and D_q in its output ports. The photons in modes B and 4 are mixed in another polarizing beam splitter in a similar way. The remaining two photons of $|\chi\rangle$ in modes 2 and 3 will serve as the output qubits.

In a CNOT gate, the value of the target qubit is to be reversed ($0\leftrightarrow1$) if the control qubit has the value 1. If the input photons in modes A and B are considered the "control" and "target" photons, respectively, then the desired CNOT gate operation corresponds to the following state transformation:

$$\alpha_1|H_A\rangle|H_B\rangle+\alpha_2|H_A\rangle|V_B\rangle+\alpha_3|V_A\rangle|H_B\rangle+\alpha_4|V_A\rangle|V_B\rangle$$
$$\rightarrow\alpha_1|H_2\rangle|H_3\rangle+\alpha_2|H_2\rangle|V_3\rangle+\alpha_3|V_2\rangle|V_3\rangle+\alpha_4|V_2\rangle|H_3\rangle$$
$$(2.1)$$

where the α are arbitrary coefficients ($\Sigma_{i=1}^{4}|\alpha_i|^2=1$), and, for example, $|H_A\rangle$ denotes a single horizontally polarized photon in mode A. From here out, the kets will be dropped from the notation for simplicity.

In Fig. 2, the partial Bell measurements at the upper and lower beam splitters simply consist of only accepting the outputs in modes 2 and 3 if one-and-only-one (1AO1) photon is detected in each of the four detectors. Combined with the polarization-dependent reflections and transmissions at the beam splitters, this condition allows the required properties of the state χ to be simply read off from the CNOT state transformation in Eq. (2.1).

For example, for the input amplitude $\alpha_1 H_A H_B$, the partial Bell measurements will only succeed if each of the photons in modes 1 and 4 are also H polarized (having one of them V polarized would result in two photons at one detector and zero at another). Furthermore, the CNOT transformation for this particular input amplitude requires the output photons in modes 2 and 3 to be H polarized, so that the state χ must contain an amplitude of the form $H_1H_4H_2H_3$.

The three remaining amplitudes may be read off in a similar manner to reveal the required form of χ:

$$\chi=\frac{1}{2}(H_1H_4H_2H_3+H_1V_4H_2V_3+V_1H_4V_2V_3$$
$$+V_1V_4V_2H_3).\qquad(2.2)$$

It can be seen from this argument that the required polarizations will be generated in the output modes whenever each of the detectors registers 1AO1 photon.

Although the above argument determines the required form of the state χ, we must also consider the way in which the output photons are entangled with the polarizations of the photons in the paths m, n, p, and q leading to the detectors. Any such entanglement would result in a more complicated
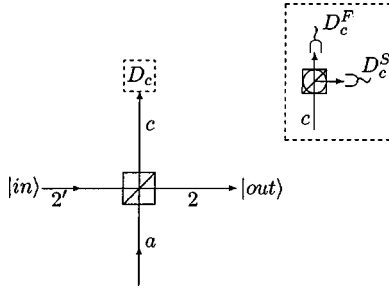
FIG. 3. Implementation of a probabilistic quantum parity check of the qubits in mode $2'$ and mode a using a polarizing beam splitter in the HV basis and a polarization-sensitive detector D_c in the FS basis. The dashed-box inset shows the details of D_c, which consists of a polarizing beam splitter in the FS basis followed by two ordinary single-photon detectors.

final state than that shown in Eq. (2.1). Roughly speaking, entanglement of this kind would provide information regarding the state of the input qubits, which would destroy the coherence of a quantum computing algorithm. This situation is analyzed in detail in the Appendix, where it is shown that this kind of information can be "erased" if each of the four detectors measure the polarization of the photons in the FS basis. This is the case because an F-polarized photon is an equal superposition of H and V polarizations, for example, so that such a measurement provides no information regarding the original values of the qubits. In this particular example, the use of a quantum erasure technique of this kind is equivalent to a $|\phi^+\rangle$ Bell-state measurement [10], but that is not the case for the more general quantum erasure operations described in Sec. III below.

It is shown in the appendix that the specified output from the detectors will be obtained 1/4 of the time, so that this CNOT gate succeeds with a probability of 25%, provided that the state χ has been created with certainty.

III. CNOT USING TWO-PHOTON ENTANGLED STATES

In this section, we describe the implementation of several kinds of probabilistic quantum logic gates using polarizing beam splitters. We then combine these elementary operations to give an implementation of a CNOT gate that does not rely upon quantum teleportation in any obvious way. In addition to providing additional insight into the nature of probabilistic quantum logic gates, this implementation may have some practical advantages in certain applications, as will be discussed in the next section. In particular, the CNOT described here uses a two-photon entangled state as a resource, rather than the four-photon entangled state required for the CNOT of the previous section.

A. Quantum parity check

The first logic operation of interest is the probabilistic quantum parity check shown in Fig. 3. The goal of this device is to transfer the value of the input qubit in mode $2'$ to the output in mode 2, provided that its value is the same as that of a second input qubit in mode a (even parity). The device fails and no output is produced if the two qubits have

different values (odd parity), and one of the qubits is destroyed in any event. The operation of this device does not measure or determine the values of either input qubit. The input and output modes have been labeled in this way to facilitate the subsequent construction of a CNOT gate. Pan *et al.* [21] have independently proposed the use of polarizing beam splitters to compare the polarization of two photons for use in entanglement purification, and similar parity checks have been proposed for other applications [22–26].

As illustrated in Fig. 3, the quantum parity check may be implemented by mixing the photons in a polarizing beam splitter and accepting the output in mode 2 only for those cases in which polarization-sensitive detector D_c receives 1AO1 photon. This may only occur if the two photons have the same polarization. In order to preserve the coherence of an arbitrary input superposition state, however, the polarization-sensitive detector D_c consists of a polarizing beam splitter oriented in the FS basis and two ordinary single-photon detectors as shown in the inset of Fig. 3.

The operation of the quantum parity check can be understood as follows: Consider an arbitrary polarization state of the input qubit $|in\rangle_{2'} = \alpha H_{2'} + \beta V_{2'}$, and a single photon in the state $|\phi_a\rangle = 1/\sqrt{2}(H_a + V_a)$. The total state, $\Psi_{2'a} \equiv |in\rangle_{2'} \otimes |\phi_a\rangle$, is transformed by the polarizing beam splitter as follows:

$$\Psi_{2'a} \rightarrow \frac{\alpha}{\sqrt{2}} H_2 H_c + \frac{\beta}{\sqrt{2}} V_2 V_c + \frac{1}{\sqrt{2}} \psi_I, \qquad (3.1)$$

where $\psi_I \equiv \alpha H_2 V_2 + \beta H_c V_c$ is composed of amplitudes that will lead to unsuccessful cases in which D_c receives two or zero photons.

Using the polarization conventions shown in Fig. 1(a) to write the mode c amplitudes in the FS basis leads to

$$\Psi_{2'a} \rightarrow \frac{1}{2} [F_c(\alpha H_2 + \beta V_2) + S_c(-\alpha H_2 + \beta V_2)] + \frac{1}{\sqrt{2}} \psi_I. \qquad (3.2)$$

From the first term inside the square brackets of Eq. (3.2), we see that if we passively accept the output only when we receive 1AO1 photon in D_c^F and zero photons in D_c^S, the arbitrary polarization of the input photon in mode $2'$ will be mapped onto the photon in mode 2 with a probability of success equal to 1/4.

Furthermore, it can be seen from the second term inside the square brackets of Eq. (3.2) that we may improve this probability from 1/4 to 1/2 if we also accept the case when we receive 1AO1 photon in D_c^S and zero photons in D_c^F. In this case however, we need to actively impart an additional phase shift that transforms mode 2 in the following way: $-\alpha H_2 + \beta V_2 \rightarrow \alpha H_2 + \beta V_2$.

Note that accepting either of these two detection outcomes does not provide any type of "which-polarization" information that would essentially serve to measure the input. Imparting the additional π phase shift could be done by rapidly changing the bias voltage on a Pockel's cell in mode 2 upon detection of a photon in D_c^S. The quantum erasure
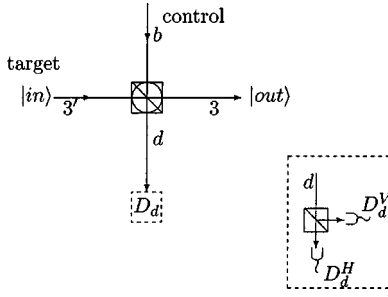
FIG. 4. Implementation of a destructive CNOT that performs a state flip on the photon in mode $3'$ that is controlled by the polarization of a single photon in mode b. Its successful operation requires the destruction of the control photon. The dashed-box inset shows the details of the polarization-sensitive detector D_d.

technique used here to eliminate any knowledge of the input qubit is not equivalent to a Bell-state measurement or to quantum teleportation, since it only involves the detection of a single photon.

B. Destructive-CNOT

A probabilistic logic device that we refer to as a destructive CNOT is shown in Fig. 4. In this device, the "target" input photon in mode $3'$ is mixed with another input photon in mode b at a polarizing beam splitter that is oriented in the FS basis. The goal of this device is to flip the polarization state (e.g., $H \leftrightarrow V$) of the "target" photon if the "control" photon in mode b is V polarized, and do nothing if it is H polarized. This operation is equivalent to a probabilistic CNOT gate except that the information contained in the control photon is destroyed in the process.

As in the quantum parity check, the output in mode 3 will only be accepted if the polarization-sensitive detector D_d (see inset box in Fig. 4) receives 1AO1 photon. The operation of Fig. 4 can be understood by first considering the case of an arbitrary polarization state of the "target" photon, $|in\rangle_{3'} = \alpha H_{3'} + \beta V_{3'}$, and a single V-polarized photon in mode b, $|\phi_b\rangle = V_b$.

Writing these states in the FS basis, the total state $\Psi_{3'b} \equiv |in\rangle_{3'} \otimes |\phi_b\rangle$ is given by

$$\Psi_{3'b} = \left[\frac{\alpha}{\sqrt{2}}(F_{3'} - S_{3'}) + \frac{\beta}{\sqrt{2}}(F_{3'} + S_{3'}) \right] \otimes \frac{1}{\sqrt{2}}(F_b + S_b). \tag{3.3}$$

The polarizing beam splitter transforms this into

$$\Psi_{3'b} \rightarrow \frac{1}{2}[\alpha(F_d F_3 - S_d S_3) + \beta(F_d F_3 + S_d S_3)] + \frac{1}{\sqrt{2}}\psi_{\mathrm{II}}, \tag{3.4}$$

where $\psi_{\mathrm{II}} \equiv \alpha/\sqrt{2}(F_3 S_3 - F_d S_d) + \beta/\sqrt{2}(F_3 S_3 + S_d F_d)$ includes the amplitudes that would lead to the unsuccessful cases in which D_d does not receive 1AO1 photon. Rewriting the amplitudes in mode d back in the HV basis leads to

$$\Psi_{3'b} \rightarrow \frac{1}{2}[H_d(\alpha V_3 + \beta H_3) + V_d(\alpha H_3 + \beta V_3)] + \frac{1}{\sqrt{2}}\psi_{\mathrm{II}}. \tag{3.5}$$

If we accept only outcomes in which detector D_d^H receives 1A01 photon and D_d^V receives zero photons, the output collapses to the state $\alpha V_3 + \beta H_3$. This corresponds to a "flip" of the input state $\alpha H_{3'} + \beta V_{3'}$ and occurs with a probability of 1/4.

From Eq. (3.5), we see that this probability can be increased to 1/2 if we also accept the outcomes in which D_d^V receives 1A01 photon and D_d^H receives zero photons. For this outcome, however, we need to apply classically controlled single-qubit operations that accomplish the transformation $\alpha H_3 + \beta V_3 \rightarrow \alpha V_3 + \beta H_3$. This could be done, for example, by first rotating the polarization of the photon in mode 3 by $90°$, and then imparting the same type of polarization dependent π-phase shift that was used in quantum parity check device.

To complete the description of the destructive-CNOT operation, we now consider the case where we have the same arbitrary state of the input "target" photon, $|in\rangle_{3'} = \alpha H_{3'} + \beta V_{3'}$, but a single H-polarized photon in mode b, $|\phi_b\rangle = H_b$. Following the steps that lead to Eq. (3.5), it can be shown that

$$\Psi'_{3'b} \rightarrow \frac{1}{2}[H_d(\alpha H_3 + \beta V_3) + V_d(\alpha V_3 + \beta H_3)] + \frac{1}{\sqrt{2}}\psi_{\mathrm{III}}, \tag{3.6}$$

where $\psi_{\mathrm{III}} \equiv \alpha/\sqrt{2}(F_3 S_3 + F_d S_d) + \beta/\sqrt{2}(F_3 S_3 - S_d F_d)$ again includes the amplitudes that lead to unsuccessful detection. In comparison with Eq. (3.5), we see that using the same detection scheme and single-qubit operations for the case of an H-polarized control photon will leave the state of the target photon unchanged.

From Eqs. (3.5) and (3.6), it is clear that the destructive CNOT performs a polarization state-flip transformation of the input photon in mode $3'$ that is controlled by the polarization of the control photon in mode b. However, this transformation is only realized by a post-selection process that destroys the control photon.

C. Quantum encoder

Although the CNOT described above destroys the control photon, such a device would still be useful if we could copy the value of the control qubit before the CNOT operation, so that all of the information would still be available after the operation was completed. With that in mind, we now describe the operation of a probabilistic quantum encoder as shown in Fig. 5. The intended function of this device is to copy (encode) the value of the input qubit in mode $2'$ into both of the output modes 2 and b. An operation of this kind is not equivalent to quantum cloning [27] and is conventionally referred to as a quantum encoder [28]. Once again, the modes have been labeled in such a way as to facilitate the subsequent construction of a CNOT.
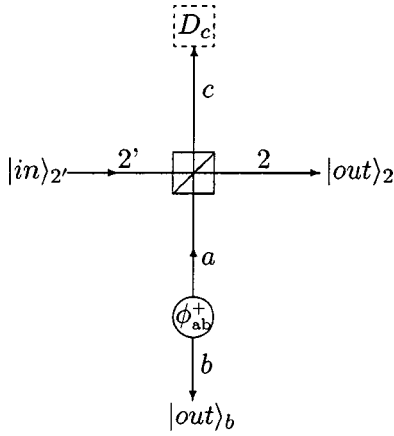
FIG. 5. A quantum encoder circuit that is identical to the quantum parity check of Fig. 3 except the single photon in mode a is now part of a two-photon Bell-state $\phi_{ab}^+ = 1/\sqrt{2}(H_a H_b + V_a V_b)$.

A quantum encoder may be implemented by combining the quantum parity check described above with a two-photon entangled state of the form $\phi_{ab}^+ = 1/\sqrt{2}(H_a H_b + V_a V_b)$, where one member of the two-photon entangled state provides the input to mode a of the quantum parity check. This is illustrated in Fig. 5, where we use the same detection scheme and single-qubit operations used in the quantum parity check.

Recall that in the quantum parity check, a successful detection event post-selected outcomes that effectively realized the transformation $\alpha H_{2'} + \beta V_{2'} \rightarrow \alpha H_2 + \beta V_2$, provided that the values of the qubits in modes a and $2'$ were the same. Based on the same arguments used to derive Eq. (3.2), it may be shown that successful detection in Fig. 5 post selects the following transformation of the same arbitrarily polarized input state:

$$\alpha H_{2'} + \beta V_{2'} \rightarrow \alpha H_2 H_b + \beta V_2 V_b. \tag{3.7}$$

As in the quantum parity check, the operation of the quantum encoder succeeds with a probability of 1/2.

It should be apparent from Eq. (3.7) that the operation of a quantum encoder is not equivalent to quantum cloning [27], even though the value of the input qubit is copied onto two output qubits. The value of the input and output qubits is not determined or measured during the operation of this device.

D. Nondestructive CNOT

The elementary logic operations described above may now be combined to implement a nondestructive CNOT gate as illustrated in Fig. 6. The quantum encoder of Fig. 5 is used to copy the value of the control qubit of mode $2'$ directly into the output in mode 2 as well as into the input mode b of the destructive-CNOT gate of Fig. 4. The output in mode 3 will then contain the result of the destructive-CNOT operation while the value of the control qubit is preserved in the other output mode. All of the mode labels have been preserved to facilitate comparisons of Figs. 4, 5, and 6.
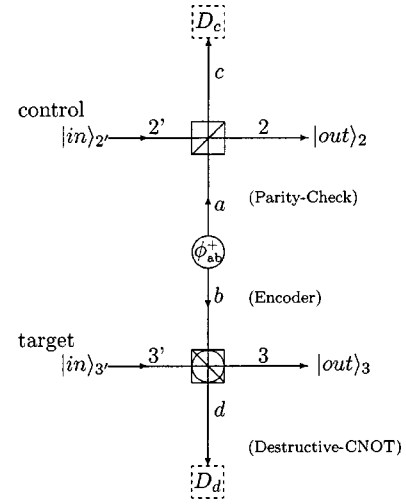

FIG. 6. Construction of a probabilistic CNOT gate by combining a quantum encoder with a destructive CNOT. The mode labels have been preserved to facilitate comparisons with Figs. 4 and 5.

Since the quantum parity check and destructive-CNOT operations both succeed with a probability of 1/2, it follows that the CNOT gate of Fig. 6 will succeed with an overall probability of 1/4. The operation of the gate may be explicitly verified by considering an arbitrary input state of the form

$$\Psi_{2'3'} = \alpha_1 H_{2'} H_{3'} + \alpha_2 H_{2'} V_{3'} + \alpha_3 V_{2'} H_{3'} + \alpha_4 V_{2'} V_{3'}, \tag{3.8}$$

and calculating the evolution of the total state $\Psi_t \equiv \Psi_{2'3'} \otimes \phi_{ab}^+$. Based on the same types of arguments used in the descriptions of the earlier logic devices, it can be shown that

$$\begin{aligned}
\Psi_t \rightarrow \frac{1}{4} \{ & F_c H_d [+\alpha_1 H_2 H_3 + \alpha_2 H_2 V_3 + \alpha_3 V_2 V_3 + \alpha_4 V_2 H_3] \\
&+ S_c H_d [-\alpha_1 H_2 H_3 - \alpha_2 H_2 V_3 + \alpha_3 V_2 V_3 + \alpha_4 V_2 H_3] \\
&+ F_c V_d [+\alpha_1 H_2 V_3 + \alpha_2 H_2 H_3 + \alpha_3 V_2 H_3 + \alpha_4 V_2 V_3] \\
&+ S_c V_d [-\alpha_1 H_2 V_3 - \alpha_2 H_2 H_3 + \alpha_3 V_2 H_3 + \alpha_4 V_2 V_3] \} \\
&+ \frac{\sqrt{3}}{2} \psi_{\text{IV}}, \tag{3.9}
\end{aligned}$$

where ψ_{IV} is a normalized combination of all of the amplitudes that would not lead to 1AO1 photon in each of the polarization-sensitive detectors D_c and D_d. The amplitudes of interest are grouped together as the four main terms inside the curly brackets of Eq. (3.9).

From the first of these four terms, we see that if we passively accept only those cases in which we receive 1AO1 photon in D_c^F and 1AO1 photon in D_d^H (e.g., the passive success conditions of the quantum parity check device and the destructive CNOT, respectively), then we accomplish the desired CNOT transformation on the input state of Eq. (3.8) with a success probability of 1/16. However, if we also accept the three other terms inside the curly brackets of Eq.

(3.9) and implement the appropriate combinations of the classically controlled single-qubit operations used in the quantum parity check and the destructive CNOT, then the four main terms all combine and increase this probability from 1/16 to 1/4.

For example, in the second term inside the curly brackets of Eq. (3.9), the detection of a single S-polarized photon in detector D_c triggers the polarization-dependent π-phase shift on mode 2 ($H_2 \rightarrow -H_2$). In the third term, the detection of a single V-polarized photon in D_d requires the state flip on the photon in mode 3 (e.g., $H_3 \leftrightarrow V_3$). Finally, we see that the fourth term inside the curly brackets of Eq. (3.9) requires both of these single-qubit operations.

The net result is that the desired CNOT operation may be performed with a probability of 1/4 without measuring or determining the values of the input qubits. The operation is known to be successful with certainty when the specified combination of detectors each registers a single photon, as is also the case for previous implementations [1,2].

IV. SUMMARY AND CONCLUSIONS

One of the main results of this paper is the probabilistic CNOT implementation shown in Fig. 6. Although our paper was inspired by Refs. [1] and [2], our CNOT in Fig. 6 differs from earlier implementations in several respects. Our implementation uses only polarizing beam splitters with total reflection or transmission, which simplifies the analysis. We showed how a CNOT gate could be constructed from more elementary operations, such as a quantum parity check, which also clarifies the operation of the resulting CNOT gate. Our approach is not directly related to quantum teleportation and depends, instead, on a quantum erasure technique. Finally, our implementation provides a higher probability of success for a given number of ancilla than is the case for the earlier implementations, and it uses half as many detectors as do several other implementations. We now discuss some of these features in more detail.

From a basic physics perspective, one conclusion from our paper is that quantum erasure may play an essential role in the implementation of a probabilistic CNOT gate. The implementation of the elementary logic operations described above were all based on the mixing of two input photons on a single beam splitter, followed by a single polarization-sensitive detector. Quantum erasure techniques were used to eliminate any information regarding the values of the two inputs. In contrast, quantum teleportation uses the output of two single-photon detectors to recreate the state of one of the original photons, as was discussed in connection with the Gottesman-Chuang protocol in Sec. II. The fundamental feature of quantum logic operations as opposed to classical logic operations is that the input qubits must remain uncertain, which can be accomplished using quantum erasure techniques.

The fundamental role of quantum erasure may be further understood by comparing our implementation in Fig. 6 with that of Koashi, Yamamoto, and Imoto [2]. Without going into any detail, our Fig. 6 bears a (superficial) resemblance to the inner portion of their implementation, in which they used four ancilla photons to generate a state analogous to the four-photon entangled state χ. They followed this by quantum teleportation of the two input qubits using two Bell-state measurements, which constituted the remainder of their implementation. Our implementation is roughly equivalent to eliminating their teleportation and Bell state measurements while replacing two of their ancilla with the actual input qubits. The net result is that our approach achieves a CNOT with a probability of 1/4 using only two ancilla, while the basic KYI implementation [2] requires four ancilla and succeeds with a probability of 1/16. Our approach also requires half as many detectors. This result may be interpreted as a more efficient use of quantum erasure without quantum teleportation.

One of the original implementations suggested by Knill, LaFlamme, and Milburn [1] also involves the generation of a four-mode entangled state analogous to χ followed by partial Bell-state measurements similar to those of Sec. II. A CNOT gate could also be implemented without teleportation using their nonlinear phase shift, which would also achieve a probability of success of 1/16 using two ancilla, whereas our implementation achieves a probability of success of 1/4 using two ancilla. As a practical matter, however, it should be noted that our implementation requires the two ancilla to be entangled whereas the KLM approach does not.

Although the CNOT scheme of Fig. 6 requires only two ancilla in contrast to the four-photon entangled state χ required for the CNOT scheme of Fig. 2, the latter approach does offer some computational advantages. For example, the reliance on four ancilla photons in the original KYI proposal [2] allows them to overcome certain problems associated with imperfect sources and photon loss. Furthermore, KLM have described a remarkable process in which the success probability of the teleportations required in a GC-like protocol may be increased arbitrarily close to one using more complex linear optics techniques [1]. In this way, they show that any GC-like protocol could, in principle, be reduced to the problem of preparing a special four-qubit state analogous to χ. The beauty of the KLM proposal is that this allows the state χ to be prepared probabilistically. Upon successful generation of χ, a GC-like protocol can then be carried out on the qubits of interest.

Within this context, it is interesting to note that the probabilistic CNOT described in Fig. 6 could itself be used to generate the state χ by a method suggested in Ref. [4] (see Fig. 7). Given a reliable source of triggered two-photon Bell states, it would require, on average, only four attempts to generate the four-photon entangled state χ. In this sense, the CNOT scheme of Fig. 6 could offer a speed up in the basic state preparation step for subsequent use in the original KLM proposal [1].

Experimental realizations of the quantum parity check, quantum encoder, and destructive-CNOT devices used to build the CNOT scheme of Fig. 6 will require reliable sources of single photons to serve as the qubits of interest, as well as reliable sources of triggered two-photon entangled states to serve as the ancilla. Several promising approaches towards generating single photons on demand are currently being investigated (see, for example [29–37]). Parametric down con-
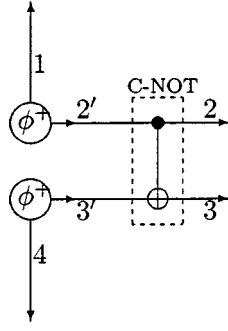
FIG. 7. GC method [4] for creation of the four-photon entangled state χ from two two-photon entangled states. Here, $\phi^+_{ij'} = 1/\sqrt{2}(H_i H_{j'} + V_i V_{j'})$, where $i, j = 1,2$ or $4,3$. The CNOT between modes $2'$ and $3'$ converts the product $\phi^+_{12'} \otimes \phi^+_{43'}$ into the four-photon state χ.

version may be used to produce entangled pairs of photons in the required Bell state, but the pairs are created at random times that cannot be determined without destroying one of the photons. Entanglement swapping [38,39] between two parametric down-conversion pairs may be used to produce heralded pairs of entangled photons, while recently discovered quantum dot techniques [40] may eventually provide a triggered source of entangled photon pairs.

In summary, we have described the operation of several photonic quantum logic devices of an elementary nature, including a quantum parity check, a quantum encoder, and a destructive-CNOT. These devices may be combined to perform a probabilistic CNOT operation on two arbitrary polarization-encoded photonic qubits. These quantum logic operations rely on linear optical elements in the form of polarizing beam splitters, additional photons (ancilla), and a post-selection process based on the outcome of single-photon detectors. Our results provide additional insight into the nature of probabilistic logic operations using linear elements and they suggest that quantum erasure techniques can play a fundamental role in these devices.

APPENDIX

In Sec. II, we introduced the basic idea behind a limited version of the GC protocol [4] that relied on polarization-encoded qubits and partial Bell measurements. In this case, the partial Bell-measurement procedure was simply to accept the output in modes 2 and 3 if and only if each of the four detectors received 1AO1 photon. That approach allowed the required properties of the special four-photon entangled state χ to be understood in a straightforward manner.

In this Appendix, we provide a more detailed analysis that includes the entanglement between the output photons and the polarizations of the photons in the modes m, n, p, and q leading to the four detectors. It will be found that this entanglement would provide information regarding the val-

ues of the input qubits unless that information is "erased" using polarization sensitive detectors in the FS basis. Furthermore, additional single-qubit operations on the output modes are required to achieve the highest possible probability of successful operation.

The initial state of the system is given by the product of the arbitrary input state, ψ_{in}, defined by the left-hand side of Eq. (2.1), and the state χ whose properties are given in Eq. (2.2)

$$\Psi_t \equiv (\alpha_1 H_A H_B + \alpha_2 H_A V_B + \alpha_3 V_A H_B + \alpha_4 V_A V_B)$$

$$\otimes \frac{1}{2}(H_1 H_4 H_2 H_3 + H_1 V_4 H_2 V_3 + V_1 H_4 V_2 V_3$$

$$+ V_1 V_4 V_2 H_3). \tag{A1}$$

Expanding Eq. (A1) and carrying out the polarizing beam-splitter transformations on the amplitudes in modes A, B, 1, and 4, results in a total of 16 amplitudes. Of these 16 amplitudes, only four correspond to a "successful" outcome in which there is 1AO1 photon in each of the four detectors; the other 12 amplitudes correspond to "unsuccessful" outcomes in which one or two detectors received two or zero photons.

It is straightforward to show that

$$\Psi_t = \frac{1}{2}\{\alpha_1 H_2 H_3 (H_p H_q H_n H_m) + \alpha_2 H_2 V_3 (H_p H_q V_n V_m)$$

$$+ \alpha_3 V_2 V_3 (V_p V_q H_n H_m) + \alpha_4 V_2 H_3 (V_p V_q V_n V_m)\}$$

$$+ \frac{\sqrt{3}}{2} \psi_V \tag{A2}$$

where the four "successful" amplitudes are explicitly shown, and ψ_V is a normalized combination of the 12 "unsuccessful" amplitudes.

The potential difficulty due to entanglement is apparent from the terms inside the curly brackets of Eq. (A2). In principle, we are able to distinguish the polarizations of the two photons in the output modes 2 and 3 based on the combinations of the polarizations of the four photons in the detection modes. This information essentially serves to measure the output, thereby spoiling the CNOT transformation of the arbitrary input state.

In order to "erase" this information [13–15] and preserve the coherence of the output amplitudes, each of the four polarization-sensitive detectors will consist of a polarizing beam splitter in the FS basis and two ordinary single-photon detectors. This type of polarization-sensitive detector is shown in the inset of Fig. 3.

We therefore write each of the detection mode amplitudes in Eq. (A2) in the FS basis. This leads to a total of 16 possible detection outcomes that correspond to the "success" condition of having 1A01 photon in each of the detector packages. It is convenient to group the amplitudes of the expansion of Eq. (A2) in terms of these 16 detection outcomes. The details are straightforward, but only the first and last two terms are shown here to save space

$$\Psi_t = \frac{1}{8}\{F_p F_q F_n F_m[+\alpha_1 H_2 H_3 + \alpha_2 H_2 V_3 + \alpha_3 V_2 V_3 + \alpha_4 V_2 H_3]$$

$$+ F_p F_q F_n S_m[-\alpha_1 H_2 H_3 + \alpha_2 H_2 V_3 - \alpha_3 V_2 V_3 + \alpha_4 V_2 H_3]$$

$$\vdots$$

$$\vdots$$

$$+ S_p S_q S_n F_m[-\alpha_1 H_2 H_3 + \alpha_2 H_2 V_3 - \alpha_3 V_2 V_3 + \alpha_4 V_2 H_3]$$

$$+ S_p S_q S_n S_m[+\alpha_1 H_2 H_3 + \alpha_2 H_2 V_3 + \alpha_3 V_2 V_3 + \alpha_4 V_2 H_3]\}$$

$$+ \frac{\sqrt{3}}{2}\psi_V. \tag{A3}$$

From the first term inside the curly brackets, we see that passively accepting only the detection outcome in that each of the four detectors receives 1AO1 F-polarized photon projects the desired CNOT transformation of the arbitrary input onto the output modes 2 and 3 with a success probability of 1/64. However, employing the same techniques described in the text for the quantum parity check and destructive CNOT, we may increase this probability by accepting the other 15 ''successful'' detection outcomes and performing classically controlled single-qubit operations to correct for the various minus signs on the amplitudes in the output modes. In this way all 16 terms contribute to the same outcome and the probability of success goes from 1/64 to 1/4.

One way to correct the minus signs in Eq. (A3) is to use a protocol in which detection of an S-polarized photon in any of the detectors activates a specific combination of polarization-dependent π-phase shifts on the output modes. For example, the following protocol will achieve the desired corrections:

$$S_p \quad \text{or} \quad S_q \Rightarrow (H_2 \rightarrow -H_2),$$

$$S_m \quad \text{or} \quad S_n \Rightarrow (H_2 \rightarrow -H_2) \quad \text{and} \quad (V_3 \rightarrow -V_3). \tag{A4}$$

These phase shifts are to be applied independently for each detector outcome. For example, if S_p and S_q outcomes are both obtained, then the sign reversal is to be applied twice, which has no net effect in that case.

[1] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).

[2] M. Koashi, T. Yamamoto, and N. Imoto, Phys. Rev. A **63**, 030301 (2001).

[3] Earlier approaches for using linear optics to simulate quantum algorithms require exponentially large resources. See, for example, N. J. Cerf, C. Adami, and P. G. Kwiat, Phys. Rev. A **57**, 1477 (1998); P. G. Kwiat, J. R. Mitchell, P. D. Schwindt, and A. G. White, J. Mod. Opt. **47**, 257 (2000).

[4] D. Gottesman and I. Chuang, Nature (London) **402**, 390 (1999).

[5] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[6] S. L. Braunstein, A. Mann, and M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992); S. L. Braunstein and A. Mann, Phys. Rev. A **51**, R1727 (1995).

[7] L. Vaidman and N. Yoran, Phys. Rev. A **59**, 116 (1999).

[8] N. Lutkenhaus, J. Calsamiglia, and K. A. Suominen, Phys. Rev. A **59**, 3295 (1999).

[9] Y. H. Kim, S. P. Kulik, and Y. H. Shih, Phys. Rev. Lett. **86**, 1370 (2001).

[10] M. Michler, K. Mattle, H. Weinfurter, and A. Zeilinger, Phys. Rev. A **53**, R1209 (1996).

[11] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).

[12] D. Bouwmeester, J. Pan, K. Mattle, H. Weinfurter, and A. Zeilinger, Nature (London) **390**, 575 (1997).

[13] M. O. Scully and K. Druhl, Phys. Rev. A **25**, 2208 (1982).

[14] P. G. Kwiat, A. M. Steinberg, and R. Y. Chiao, Phys. Rev. A **45**, 7729 (1992).

[15] T. J. Herzog, P. G. Kwiat, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **75**, 3034 (1995).

[16] These axes have been designated F and S in analogy with the fast and slow axes of birefringent crystals. In this paper, however, the HV and FS bases are equivalent.

[17] H. Fearn and R. Loudon, J. Opt. Soc. Am. B **6**, 917 (1989).

[18] M. Zukowski, A. Zeilinger, and H. Weinfurter, Ann. N.Y. Acad. Sci. **755**, 91 (1995); A. Zeilinger, M. A. Horne, H. Weinfurter, and M. Zukowski, Phys. Rev. Lett. **78**, 3031 (1997).

[19] Z. Y. Ou, Quantum Semiclassic. Opt. **9**, 599 (1997).

[20] J. G. Rarity, P. R. Tapster, and R. Loudon, e-print quant-ph/9702032.

[21] J. W. Pan, C. Simon, C. Brukner, and A. Zeilinger, Nature (London) **410**, 1067 (2001).

[22] J. W. Pan and A. Zeilinger, Phys. Rev. A **57**, 2208 (1998).

[23] J. W. Pan, M. Daniell, S. Gasparoni, G. Weihs, and A.

Zeilinger, Phys. Rev. Lett. **86**, 4435 (2001).

[24] D. Bouwmeester, Phys. Rev. A **63**, 040301 (2001).

[25] T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. A **64**, 012304 (2001).

[26] Z. Zhao, J. W. Pan, and M. S. Zhan, Phys. Rev. A **64**, 014301 (2001).

[27] W. K. Wooters and W. H. Zurek, Nature (London) **299**, 802 (1982).

[28] *Quantum Computing and Quantum Information*, M. A. Nielsen and I. L. Chuang (Cambridge University Press, Cambridge, MA, 2000).

[29] H. J. Kimble, M. Dagenais, and L. Mandel, Phys. Rev. Lett. **39**, 691 (1977).

[30] C. K. Hong and L. Mandel, Phys. Rev. Lett. **56**, 58 (1986).

[31] F. DeMartini, G. DiGiuseppe, and M. Marrocco, Phys. Rev. Lett. **76**, 900 (1996).

[32] J. Kim, O. Benson, H. Kan, and Y. Yamamoto, Nature (London) **397**, 500 (1999).

[33] P. Michler, A. Imamoglu, M. D. Mason, P. J. Carson, G. F. Strouse, and S. K. Buratto, Nature (London) **406**, 968 (2000); P. Michler, A. Kiraz, C. Becher, W. V. Schoenfeld, P. M. Petroff, L. Zhang, E. Hu, and A. Imamoglu, Science **290**, 2282 (2000).

[34] C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter, Phys. Rev. Lett. **85**, 290 (2000).

[35] R. Brouri, A. Beveratos, J. P. Poizat, and P. Grangier, Opt. Lett. **25**, 1294 (2000).

[36] B. Lounis and W. E. Moerner, Nature (London) **407**, 491 (2000).

[37] S. Brattke, B. T. H. Varcoe, and H. Walther, Phys. Rev. Lett. **86**, 3534 (2001).

[38] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).

[39] J. W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).

[40] O. Benson, C. Santori, M. Pelton, and Y. Yamamoto, Phys. Rev. Lett. **84**, 2513 (2000).