PHYSICAL REVIEW A, VOLUME 63, 030301(R)

Probabilistic manipulation of entangled photons

Masato Koashi, Takashi Yamamoto, and Nobuyuki Imoto

CREST Research Team for Interacting Carrier Electronics, School of Advanced Sciences, The Graduate University for Advanced Studies (SOKEN), Hayama, Kanagawa, 240-0193, Japan

(Received 16 October 2000; published 12 February 2001)

We propose probabilistic controlled-NOT and controlled-phase gates for qubits stored in the polarization of photons. The gates are composed of linear optics and photon detectors, and consume polarization entangled photon pairs. The fraction of the successful operation is only limited by the efficiency of the Bell-state measurement. The gates work correctly under the use of imperfect detectors and lossy transmission of photons. Combined with single-qubit gates, they can be used for producing arbitrary polarization states and for designing various quantum measurements.

DOI: 10.1103/PhysRevA.63.030301 PACS number(s): 03.67.Lx, 42.50.−p

Entanglement plays an important role in various schemes of quantum information processing, such as quantum teleportation [1], quantum dense coding [2], certain types of quantum key distributions [3], and quantum secret sharing [4]. It is natural to expect that entanglement shared among many particles will be useful for more complicated applications including communication among many users. Among the physical systems that can be prepared in entangled states, photons are particularly suited for such applications because they can easily be transferred to remote places. Several schemes for creating multiparticle entanglement from a resource of lower numbers of entangled particles have been proposed [5,6], and experimentally a three-particle entangled state [a Greenberger-Horne-Zeilinger (GHZ) state] was created from two entangled photon pairs [7].

In order to synthesize *any* states of *n* photons on demand, the concept of quantum gates is useful. The universality of the set of the controlled-NOT gate and single-qubit gates [8,9] implies that you can create any states by making a quantum circuit using such gates. In addition to synthesizing quantum states, this scheme also enables general transformation and generalized measurement in the Hilbert space of *n* photons. A difficulty in this strategy is how to make two photons interact with each other and realize two-qubit gates. One way to accomplish this is to implement conditional dynamics at the single-photon level through the strong coupling to the matter such as an atom, and a demonstration has been reported [10], which is a significant step toward this goal. On the other hand, if we restrict our tools to linear optical elements, a never-failing controlled-NOT gate is impossible, which is implied by the no-go theorem for Bell-state measurements [11]. It is, however, still possible to construct a ''probabilistic gate,'' which tells us whether the operation has been successful or not and do the desired operation faithfully for the successful cases. While the probabilistic nature hinders the use for the fast calculation of classical data that outruns classical computers, such a gate will still be a useful tool for the manipulation of quantum states of a modest number of photons, because no classical computer can be a substitute for this purpose.

In this Rapid Communication, we propose probabilistic two-qubit gates for qubits stored in the polarization of photons. The gates are composed of photon detectors and linear optical components such as beam splitters and wave plates. As resources, the gates consume entangled photon pairs. When the detectors with quantum efficiency η are used, the success probability of $\eta^4/4$ can be obtained, which is only limited by the efficiency of the Bell measurement used in the scheme. Combined with single-qubit gates that are easily implemented by linear optics, the proposed gates can build quantum circuits conducting arbitrary unitary operations with nonzero success probabilities.

In Fig. 1 we show the schematic of scheme I, the simplest of the schemes we propose in this paper. The gate requires two photons and a pair of photons in a Bell state as resources. Initially, they are in the states $|H\rangle_{2a}$, $|H\rangle_{2b}$, and $(|H\rangle_{3a}|V\rangle_{3b}-|V\rangle_{3a}|H\rangle_{3b})/\sqrt{2}$. The wave plate WP5 rotates the polarization of mode $3a$ by 45°, namely, $|H\rangle_{3a}\to(|H\rangle_{3'a}+|V\rangle_{3'a})/\sqrt{2}$ and $|V\rangle_{3a}\to(|H\rangle_{3'a}-|V\rangle_{3'a})/\sqrt{2}$. After WP5, the entangled photon pair becomes

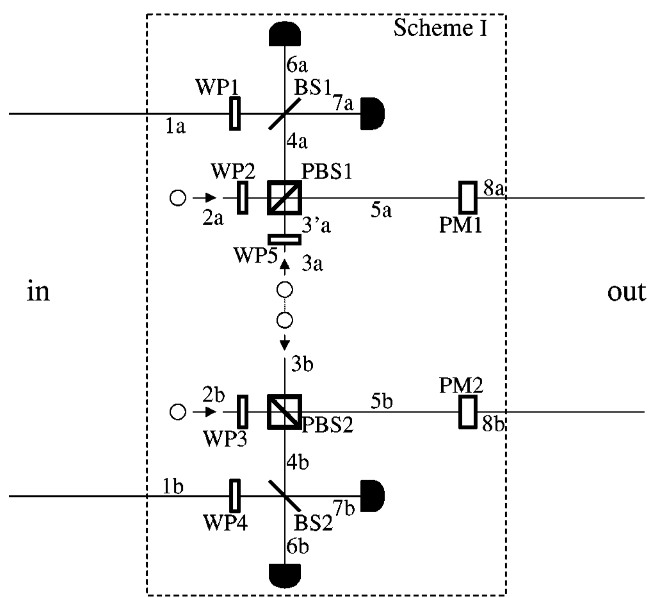

FIG. 1. Schematic of the setup of a controlled-phase gate (scheme I).

$$\frac{1}{2}(|V\rangle_{3'a}|V\rangle_{3b}+|H\rangle_{3'a}|V\rangle_{3b}+|V\rangle_{3'a}|H\rangle_{3b}-|H\rangle_{3'a}|H\rangle_{3b}). \tag{1}$$

The polarizing beam splitter PBS1 transmits H photons and reflects V photons. Combined with WP2, it gives the transformation $|H\rangle_{2a}|H\rangle_{3'a}\to(|H\rangle_{4a}|H\rangle_{5a}+|V\rangle_{4a}|H\rangle_{4a})\sqrt{2}$ and $|H\rangle_{2a}|V\rangle_{3'a}\to(|V\rangle_{4a}|V\rangle_{5a}+|H\rangle_{5a}|V\rangle_{5a})\sqrt{2}$. Photons in the b modes are similarly transformed, and we obtain the state

$$(\beta/2)(|V\rangle_{4a}|V\rangle_{4b}|V\rangle_{5a}|V\rangle_{5b}+|H\rangle_{4a}|V\rangle_{4b}|H\rangle_{5a}|V\rangle_{5b} +|V\rangle_{4a}|H\rangle_{4b}|V\rangle_{5a}|H\rangle_{5b}-|H\rangle_{4a}|H\rangle_{4b}|H\rangle_{5a}|H\rangle_{5b}) + \sqrt{1-\beta^2}|\phi\rangle\equiv\beta|\Psi\rangle+\sqrt{1-\beta^2}|\phi\rangle, \tag{2}$$

where $\beta=1/2$, and $|\phi\rangle$ is a normalized state in which the number of photons in mode $4a$ or mode $4b$ is not unity.

The photon in the input mode $1a$ ($1b$) passes through wave plate WP1 (WP4), which rotates its polarization by 90°, and is mixed with the photon in mode $4a$ ($4b$) by a 50/50 polarization-independent beam splitter BS1(BS2). After the beam splitters, the photon number of each mode and each polarization is measured by a photon counter. Let us assume that the state of the input qubits is

$$\alpha_1|V\rangle_{1a}|V\rangle_{1b}+\alpha_2|V\rangle_{1a}|H\rangle_{1b}+\alpha_3|H\rangle_{1a}|V\rangle_{1b} +\alpha_4|H\rangle_{1a}|H\rangle_{1b}. \tag{3}$$

The total state after the beam splitter can be calculated straightforwardly, but we do not write down the whole since it is too lengthy. We focus on the terms in which one H photon is found in modes $6a$ or $7a$, one V photon is found in modes $6a$ or $7a$, and similar conditions hold for b modes. There are 16 such combinations. For example, the terms including $|V\rangle_{6a}|H\rangle_{7a}|V\rangle_{6b}|H\rangle_{7b}$ are found to be

$$-\frac{\beta}{8}|V\rangle_{6a}|H\rangle_{7a}|V\rangle_{6b}|H\rangle_{7b}(-\alpha_1|V\rangle_{5a}|V\rangle_{5b}+\alpha_2|V\rangle_{5a}|H\rangle_{5b} +\alpha_3|H\rangle_{5a}|V\rangle_{5b}+\alpha_4|H\rangle_{5a}|H\rangle_{5b}), \tag{4}$$

and the terms including $|V\rangle_{6a}|H\rangle_{6a}|V\rangle_{7b}|H\rangle_{7b}$ are

$$\frac{\beta}{8}|V\rangle_{6a}|H\rangle_{6a}|V\rangle_{7b}|H\rangle_{7b}(-\alpha_1|V\rangle_{5a}|V\rangle_{5b}-\alpha_2|V\rangle_{5a}|H\rangle_{5b} -\alpha_3|H\rangle_{5a}|V\rangle_{5b}+\alpha_4|H\rangle_{5a}|H\rangle_{5b}). \tag{5}$$

As seen in these examples, the state in modes $5a$ and $5b$ depends on the photon distribution in modes 6 and 7. However, it is easy to check that this dependence is canceled if we introduce a phase shift by phase modulator PM1, $|H\rangle_{5a}\to|H\rangle_{8a}$ and $|V\rangle_{5a}\to-|V\rangle_{8a}$, only for the cases of $|V\rangle_{6a}|H\rangle_{6a}$ and $|V\rangle_{7a}|H\rangle_{7a}$, and similar operation for PM2. Then, for all 16 combinations, the state in modes $8a$ and $8b$ becomes

$$-\alpha_1|V\rangle_{8a}|V\rangle_{8b}+\alpha_2|V\rangle_{8a}|H\rangle_{8b}+\alpha_3|H\rangle_{8a}|V\rangle_{8b} +\alpha_4|H\rangle_{8a}|H\rangle_{8b}. \tag{6}$$

The evolution from Eq. (3) to Eq. (6) shows that this scheme operates as a controlled-phase gate if we assign $|0\rangle=|H\rangle$ and $|1\rangle=|V\rangle$. The probability of obtaining these results is $\beta^2/4=1/16$. The factor of 1/4 appearing here can be understood as due to the twofold use of Bell-state measurement schemes with 50% success probability, used in the dense coding experiment [12]. If we place two additional wave plates in modes $1b$ and $8b$, which rotate polarization by 45° and $-45°$, respectively, we obtain a probabilistic controlled-NOT gate.

Next, we consider the effect of imperfect quantum efficiency of photon detectors. In order to characterize the behavior of the detector, we introduce the parameter η_2 in addition to the quantum efficiency η, in such a way that it detects two photons with probability $\eta^2\eta_2$ when two photons simultaneously arrive. For example, conventional avalanche photodiodes (APDs) have $\eta_2=0$ since they cannot distinguish two-photon events from one-photon events. Use of N conventional APDs after beam splitting the input to N branches leads to an effective value of $\eta_2=1-1/N$. Recently, a detector with high η and with clearly distinguishable signals for one- and two-photon events was also demonstrated [13].

There are two distinctive effects caused by the imperfect quantum efficiency. The first one is that the detectors report some successful events as false ones by overlooking incoming photons. The success probability of 1/16 in the ideal case thus reduces to $p_{\mathrm{true}}^{(\mathrm{I})}\equiv\eta^4/16$. The second effect is that the detectors report some failing events as successful ones. This may occur when two photons enter mode $4a$ or $4b$, hence the output mode $8a$ or $8b$ has no photon. After some simple algebra, the probability $p_{\mathrm{false}}^{(\mathrm{I})}$ of this occurrence is obtained as $p_{\mathrm{false}}^{(\mathrm{I})}=\eta^4(3-\kappa)(1-\kappa)/4$, with $\kappa\equiv\eta(1+\eta_2)/2$. Because of this effect, after discarding the failing events indicated by the results of the photon detection, the output of the gate still includes errors at probability $p_{\mathrm{err}}^{(\mathrm{I})}\equiv p_{\mathrm{false}}^{(\mathrm{I})}/(p_{\mathrm{true}}^{(\mathrm{I})}+p_{\mathrm{false}}^{(\mathrm{I})})$. In the following, we describe two methods for removing these errors.

The first method is the postselection that is applicable when every output qubit of the whole quantum circuit is eventually measured by photon detectors. As we have seen, the errors in the gate always accompany the loss of photons in the output. We also observe easily that if the input mode $1a$ ($1b$) is initially in the vacuum state, the output mode $8a$ ($8b$) has no photon whenever the detectors show successful outcomes. This implies that if one of the gates in the circuit causes errors, at least one photon is missing in the final state of the whole circuit. The errors can thus be discarded by postselecting the events of every detector at the end of the circuit registering a photon. This method also works when the Bell-state source fails to produce two photons reliably and emits fewer photons on occasion.

The second method is to construct more reliable gates, using scheme I for the initialization processes, as shown in Fig. 2(a). This method is advantageous when the Bell-state source is close to ideal and good optical delay lines are available. In scheme II, we use two Bell pairs of photons in the state $(|H\rangle|H\rangle-|V\rangle|V\rangle)/\sqrt{2}$, and operate the conditional-

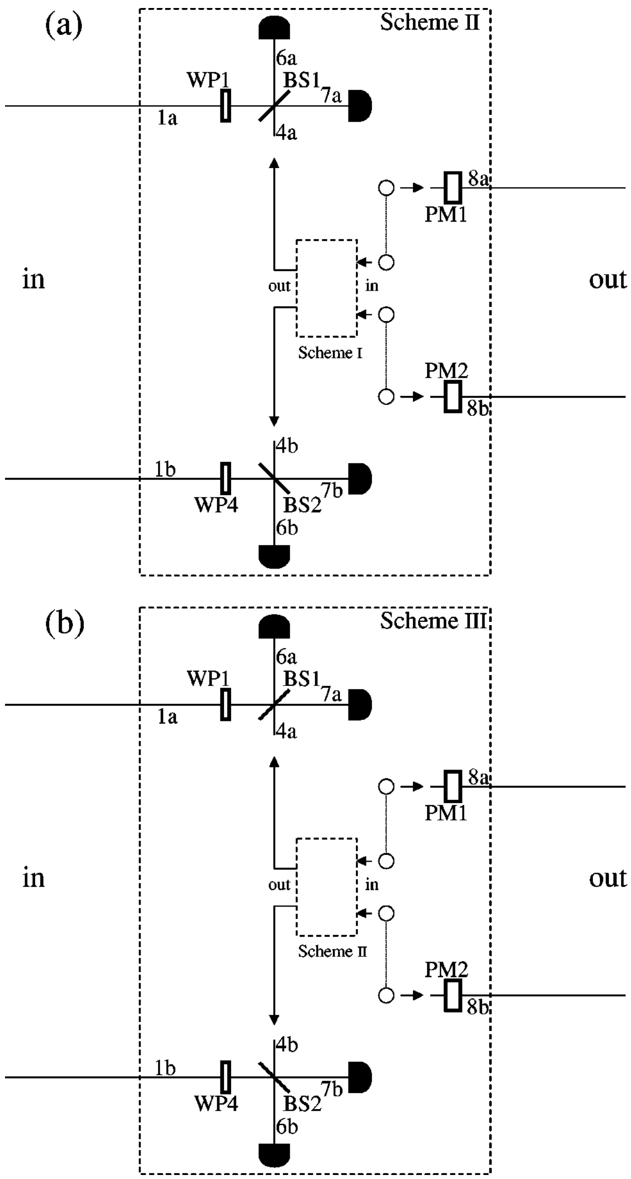

FIG. 2. Schematic of the setup of controlled-phase gates. (a) Scheme II. The gate uses scheme I inside. (b) Scheme III. The gate uses scheme II inside.

phase gate (scheme I) on the two photons, one from each pair. If the operation fails, we discard everything and retry from the start. The initialization process is complete when the operation of scheme I is successful, and the outputs are sent to modes $4a$ and $4b$. The remaining photons of Bell pairs are sent to modes $5a$ and $5b$. At this point, the quantum state is prepared in the following mixed state:

$$(1-p_{\rm err}^{(\rm I)})|\Psi\rangle\langle\Psi|+p_{\rm err}^{(\rm I)}\hat{\rho}, \tag{7}$$

where $\hat{\rho}$ is a normalized density operator representing a state in which no photon exists in mode $4a$ or $4b$. After this point, the operation of scheme II follows that of scheme I. The crucial difference from scheme I is that the state $\hat{\rho}$ has no chance to produce successful outcomes. This leads to $p_{\rm false}^{(\rm II)}=p_{\rm err}^{(\rm II)}=0$, namely, the faithful operation is obtained with the success probability of $p_{\rm true}^{(\rm II)}=(1-p_{\rm err}^{(\rm I)})\,\eta^4/4$. When one of the input modes is in the vacuum, this gate never reports the successful operation. This implies that errors caused by the loss of photons in the upstream circuit are detected and hence discarded.

Using scheme II for the initializing process, we can enhance the success probability. Scheme III shown in Fig. 2(b) is exactly the same as scheme II, except that scheme I inside is replaced by scheme II itself. When the initialization is completed, the gate inside produces exactly the state $|\Psi\rangle$. For this scheme, the probability of a successful operation is $p_{\rm true}^{(\rm III)}=\eta^4/4$, and in the ideal case it is 1/4. This limitation stems from the success probability (50% each) of the two Bell-state measurements. It should be noted that the maximum of this probability is still an open question, and if a more efficient way of Bell measurement is discovered, it will be used in our scheme to enhance the success probability of the gate.

Scheme III can be viewed as a particular implementation of the general scheme of constructing quantum gates using the concept of teleportation and Bell measurement [14], to the case of qubits stored in photons. In the general argument that considers the use of single-qubit gates, three-particle entangled states (GHZ states) are required as resources. What was shown here is that linear optical components for qubits made of photons have more functions than the single-qubit gates, and the resource requirement is further reduced to two-particle entanglement.

Since the set of the controlled-NOT gate and single-qubit gates is universal [8,9], any unitary transformation can be realized with a nonzero success probability by quantum circuits composed of the proposed gates and linear optical components. For the tasks that take classical data as an input and return classical data as an output, the quantum circuits here will not surpass the conventional classical computers due to the probabilistic nature. But there are other applications in which either the input or the output includes quantum states. For instance, they can be used as a quantum-state synthesizer, which produces any quantum state on the polarization degree of freedom with a nonzero probability. They are also used as designing various types of quantum measurement. For any positive operator valued measure (POVM) [15] given by the set of positive operators $\{F_1,\ldots,F_n\}$ with $\Sigma_k F_k=\mathbf{1}$, it is possible to realize a POVM given by $\{pF_1,\ldots,pF_n,(1-p)\mathbf{1}\}$, where p is a nonzero probability of success. As transformers of quantum states, they may be used for the purification protocol of entangled pairs [16]. This implies that if reliable resources of entangled photon pairs are realized, it may be possible to produce maximally entangled pairs shared by remote places connected only by noisy channels.

Finally, we would like to mention the requirement on the property of the entangled-pair resources. While the mixing of fewer-photon states can be remedied as discussed before, the mixing of excess photons leads to errors that are difficult to correct. For example, the photon-pair source by parametric down-conversion of coherent light with a pair production probability of $\eta_{\rm PDC}$ emits two pairs with the probability of $O(\eta_{\rm PDC}^2)$. This portion causes severe effects when the two or more gates are connected in series. The recent proposal for the regulated entangled photon pairs from a quantum dot [17] seems to be a promising candidate for the resources of the proposed gates.

Note added in proof. Recently,a proposal of quantum gates for photons, which is aimed at fast computation, was mde by Knill *et al.* [18].

This work was supported by a Grant-in-Aid for Encouragement of Young Scientists (Grant No. 12740243) by the Japan Society of the Promotion of Science.

[1] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).
[2] C. H. Bennett and S. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] M. Hillery *et al.*, Phys. Rev. A **59**, 1829 (1999).
[5] A. Zeilinger, M. A. Horne, H. Weinfurter, and M. Żukowski, Phys. Rev. Lett. **78**, 3031 (1997).
[6] S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 812 (1998).
[7] D. Bouwmeester *et al.*, Phys. Rev. Lett. **82**, 1345 (1999).
[8] T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).
[9] A. Barenco *et al.*, Phys. Rev. A **52**, 3457 (1995).
[10] Q. A. Turchette *et al.*, Phys. Rev. Lett. **75**, 4710 (1995).
[11] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, Phys. Rev. A **59**, 3295 (1999).
[12] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).
[13] J. Kim, S. Takeuchi, and Y. Yamamoto, Appl. Phys. Lett. **74**, 902 (1999).
[14] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).
[15] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993).
[16] C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996).
[17] O. Benson, C. Santori, M. Pelton, and Y. Yamamoto, Phys. Rev. Lett. **84**, 2513 (2000).
[18] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).