Repeat-until-success quantum computing using stationary and flying qubits

Yuan Liang Lim,[1] Sean D. Barrett,[2] Almut Beige,[1] Pieter Kok,[2] and Leong Chuan Kwek[3,4]
[1]*Blackett Laboratory, Imperial College London, Prince Consort Road, London SW7 2BZ, United Kingdom*
[2]*Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS34 8QZ, United Kingdom*
[3]*National Institute of Education, Nanyang Technological University, Singapore 63 9798, Singapore*
[4]*Department of Physics, National University of Singapore, Singapore 11 7542, Singapore*
(Received 29 August 2005; published 9 January 2006)

We introduce an architecture for robust and scalable quantum computation using both stationary qubits (e.g., single photon sources made out of trapped atoms, molecules, ions, quantum dots, or defect centers in solids) and flying qubits (e.g., photons). Our scheme solves some of the most pressing problems in existing nonhybrid proposals, which include the difficulty of scaling conventional stationary qubit approaches, and the lack of practical means for storing single photons in linear optics setups. We combine elements of two previous proposals for distributed quantum computing, namely the efficient photon-loss tolerant build up of cluster states by Barrett and Kok [Phys. Rev. A **71**, 060310(R) (2005)] with the idea of repeat-until-success (RUS) quantum computing by Lim *et al.* [Phys. Rev. Lett. **95**, 030505 (2005)]. This idea can be used to perform eventually deterministic two qubit logic gates on spatially separated stationary qubits via photon pair measurements. Under nonideal conditions, where photon loss is a possibility, the resulting gates can still be used to build graph states for one-way quantum computing. In this paper, we describe the RUS method, present possible experimental realizations, and analyze the generation of graph states.

DOI: 10.1103/PhysRevA.73.012304 PACS number(s): 03.67.Lx, 42.50.Dv

I. INTRODUCTION

Quantum computing offers a way to realize certain algorithms exponentially more efficiently than with the best known classical solutions [1,2]. A substantial effort has therefore been made to develop the corresponding quantum technologies. Proof-of-principle experiments demonstrating the feasibility of quantum computing have already been performed. Using nuclear magnetic resonance techniques, Vandersypen *et al.* [3] realized a simple instance of Shor's algorithm by factoring $15=3\times5$. A two-qubit gate has been implemented in a color center in diamond utilizing the electron spin state of the nitrogen vacancy defect center together with a nearby nuclear spin as qubits [4]. Groups in Innsbruck and Boulder implemented a universal two-qubit gate in an ion trap [5,6], and the three-qubit teleportation protocol [7,8]. Adding more qubits to this "proto quantum computer" will increase the density of the motional states used for the two-qubit interaction. Consequently, it will become even harder to implement clean two-qubit gates. Scaling ion trap quantum computers much further therefore seems to require some form of distributed quantum information processing, possibly involving ion transport [9].

The schemes mentioned above are based on manipulating *stationary* qubits such as atoms, molecules, or trapped ions. An alternative route to finding a feasible and scalable technology for building quantum computers is based on *flying* qubits, such as photons. The main advantage of photons is their extremely long coherence time. In vacuum and in simple dielectric media, photons do not interact with their environment, and hence do not lose their quantum information. This is why photons are usually the qubits of choice for quantum communication [10,11]. However, at the same time this lack of interaction means that it is very hard to create two-photon entangling gates. It therefore came as a surprise that the bosonic symmetry requirement of the electromagnetic field, together with photon counting and proper single-photon sources, is sufficient for implementing scalable quantum computing [12]. The overhead cost for linear optical quantum computing (LOQC) has subsequently been brought down significantly. In particular, the one-way or cluster-state model for quantum computing [13] has allowed for drastic improvements in the scalability [14–16]. Recently, a four-qubit cluster state was realized experimentally by Walther *et al.* [17]. The main drawbacks of LOQC are the difficulties of maintaining interferometric stability, the lack of practical "on demand" single-photon sources, and the lack of quantum memories for photonic qubits [18].

In this paper, we consider the practical advantage of combining stationary and flying qubits for the realization of scalable quantum computing. The stationary qubits (single photon sources) are arranged in a network of nodes with each node processing and storing a small number of qubits. To achieve scalability, the concept of distributed quantum computing was introduced and it was proposed that distant qubits communicate with each other through the means of flying qubits (i.e., photons) [19,20]. Initial schemes for the implementation of this idea relied on entangled ancillas as a resource [19–23]. Others required that the photon from one source is fed into another source [24–29] or a photon-mediated interaction between two fiber-coupled distant cavities needed to be established [30]. More hybrid approaches to quantum computing can be found in Refs. [31,32].

Other authors developed schemes for the probabilistic generation of highly entangled states between distant single photon sources [33–41]. In these schemes, one generates a photon in each of the sources and then performs an entangling photon measurement. By virtue of entanglement swapping, this results in entangled stationary qubits. It has been shown that similar ideas can also result in the implementa-

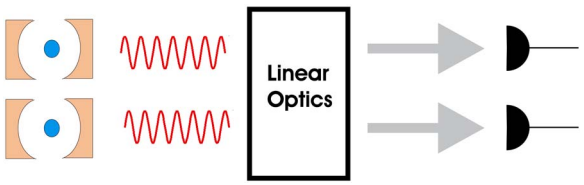

FIG. 1. (Color online) Experimental realization of a universal two-qubit gate for the considered network of single photon sources (stationary qubits). This requires the generation of a photon within each of the sources involved. The two photons then pass within their coherence time through a linear optics network which performs a certain photon pair measurement.

tion of probabilistic remote two-qubit gates [42]. At this point, it was believed that scalable quantum computing with distant photon sources requires additional resources such as local entangling gates [22] or entangled ancillas in order to become deterministic.

The concrete setup that we consider in this paper has recently been introduced by Lim *et al.* [43] and allows for the more efficient implementation of universal two-qubit gates than previous proposals. The presented scheme consists of a network of single stationary qubits (like trapped atoms, molecules, ions, quantum dots, and nitrogen vacancy color centers) inside optical cavities, which act as a source for the generation of single photons on demand. Readout measurements and single qubit rotations can be performed on the stationary qubits using laser pulses and standard quantum optics techniques as employed in the recent ion trap experiments in Innsbruck and Boulder [5,6].

The main building block for the realization of a two-qubit gate, which qualifies the setup for universal quantum computing, is shown in Fig. 1. It requires the simultaneous generation of a photon in each source involved in the operation. Afterwards the photons should pass through a linear optics setup, where a pair measurement is performed in the output ports. This photon pair measurement results either in the completion of the gate or indicates the presence of the original qubits. In the later event, the gate should be repeated. The qubits are never lost in the computation and the presented scheme is therefore called *repeat-until-success* quantum computing [43].

Under realistic conditions, i.e., in the presence of finite detector efficiencies and finite success rates for the generation of a single photon on demand, the setup in Fig. 1 can still be used for the implementation of probabilistic gates with a very high fidelity. As shown recently by Barrett and Kok [44], it is possible to use probabilistic gates to efficiently generate graph states for one-way quantum computing [13]. Both schemes, [43,44], overcome the limitations to scalable quantum computing faced before when using the same resources. In Ref. [43] this is achieved with an eventually deterministic gate. Reference [44] introduced a so-called double-heralding scheme, in which the entangling photodetection stage was employed twice to eliminate unwanted separable contributions to the density matrix.

In this paper, we combine the ideas presented in our previous work [43,44]. In this way, we obtain a truly scalable design for quantum computing, i.e., even in the presence of imperfect components, with several key advantages.

(1) Since our system uses *no direct qubit-qubit interactions*, the qubits can be well isolated. Not only does this allow us to address the individual qubits easily, it also means that there are fewer decoherence channels and hence fewer errors in the computation.

(2) We achieve *robustness to photon loss*. In the presence of photon loss, the two-qubit gates become nondeterministic. However, the gate failures are heralded, and so the gates can still be used to build high-fidelity entangled states, albeit in a nondeterministic manner. Photon loss thus increases the overall overhead cost associated with the scheme, but does not directly reduce the fidelity of the computation. When realistic photodetectors and optical elements are used, photon loss is inevitable and this built-in robustness is essential.

(3) Our scheme largely relies only on *components that have been demonstrated in experiments* like atom photon entanglement [45,46]. Apart from linear optics, we require only relatively good sources for the generation of single photons on demand [47–51], preferrably at a high rate [52], and relatively efficient but not necessarily number resolving photon detectors [53]. Combining these in a working quantum computer will be challenging, but the basic physics has been shown to be correct.

(4) The photon pair measurement is *interferometrically stable*. Since each generated photon contributes equally to the detection of a photon in the linear optics setup, fluctuations in the length between the photon source and the detectors can at most result in an overall phase factor with no physical consequences. This constitutes a significant advantage compared to previous schemes based on one-photon measurements (the only interferometrically stable schemes are [36,38,39,43]), since the photons do not need to arrive simultaneously in the detectors as long as they overlap within their coherence time in the setup.

(5) The basic ideas presented in this paper are *implementation independent* and the stationary qubits can be realized in a variety of ways. Any system with the right energy level structure and able to produce encoded flying qubits may be used.

(6) Our scheme is inherently *distributed*. Hence, it can be used in applications which integrate both quantum computation and quantum communication. We show that entanglement can be generated directly between any two stationary qubits in the physical quantum computer. This significantly reduces the computational cost compared to architectures involving only nearest-neighbor interactions between the qubits [54].

This paper is organized as follows. In the next section, we give an overview on the basic principles of measurement-based quantum computing, since the described hybrid approach to quantum computing constitutes an implementation of these ideas. Section III details the general principle of a remote two-qubit gate implementation. In Sec. IV we discuss possible gate implementations with polarization and time-bin encoded photons. In Sec. V we describe how to overcome imperfections of inefficient photon generation and detection with the help of prefabricated graph states. Finally, we state our conclusions in Sec. VI.

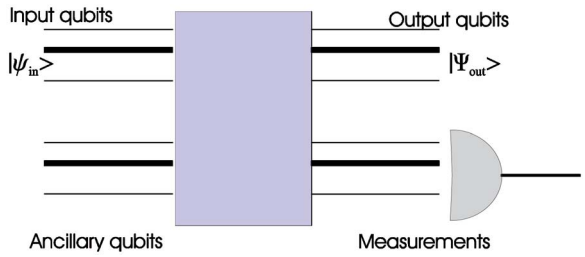

FIG. 2. (Color online) Measurement-based quantum computing. The input state $|\Psi\rangle_s$ and the auxiliary state $|A_0\rangle_a$ are transformed in an N port that induces a unitary transformation U_{sf}. Given a detector outcome corresponding to a POVM $\hat{B}_k$, the output state is $|\Upsilon_k\rangle_s$.

II. MEASUREMENT-BASED QUANTUM COMPUTING

One condition for the successful implementation of a measurement-based quantum gate is that the measurement outcome is *mutually unbiased* [55] with respect to the computational basis. In this way, an observer does not learn anything about the state of the qubits and the information might remain stored inside the computer. To avoid the destruction of qubits, it is not allowed to measure on the qubits directly. Measurements should only be performed on ancillas, which have interacted and therefore share entanglement with the qubits. These ancillas can be of the same physical realization as the computational qubits [13,56–58] but they might also be realized differently. If the stationary qubits are atoms, the ancilla can be the quantized field mode inside an optical cavity [59], a common vibrational mode [60] or newly generated photons, as in the setup considered here. Vice versa, it has been found advantageous to use collective atomic states as ancillas for photonic qubits [31,32].

Let us now briefly describe the principles of measurement-based quantum computing in a more formal way. Using the terms "qubits" and "ancillas" provides a convenient picture, which is especially suited for the description of hybrid approaches, where the qubits may remain encoded in the same physical qubits instead of being assigned dynamically as the computation proceeds. As in Ref. [61], we consider two systems, s and a, that are initially in the state ($c_n \in \mathbb{C}$)

$$|\Psi\rangle_s|A_0\rangle_a \equiv \sum_n c_n|\psi_n\rangle_s \otimes |A_0\rangle_a. \tag{1}$$

After some interaction, the joint system evolves into

$$|\Psi\rangle_s|A_0\rangle_a \to \sum_n c_n|\psi_n\rangle_s \otimes |A_n\rangle_a \equiv |\Phi\rangle, \tag{2}$$

where the $|A_n\rangle_a$ are the eigenstates of an observable A. We can then measure A, which will reveal the state of the system s. This can be interpreted as a quantum nondemolition measurement of s but this is not what we are interested in here.

In this paper we will instead consider measurements of an observable B, as shown in Fig. 2, that is complementary to A. In other words, the eigenvectors of A and B form a so-called mutually unbiased basis of the Hilbert space of system s. A specific outcome labeled k of such a measurement corresponds to the application of the projection operator $\hat{B}_k$ (associated with the kth eigenvector of B), and the state of system s is then given by

$$|\Upsilon_k\rangle_s = \frac{\mathrm{Tr}_a[\langle\Phi|\mathbb{1}\otimes\hat{B}_k|\Phi\rangle]}{\mathrm{Tr}_{sa}[\langle\Phi|\mathbb{1}\otimes\hat{B}_k|\Phi\rangle]}. \tag{3}$$

This can be generalized to situations where $\hat{B}_k$ is a multirank projector or a positive operator valued measure (POVM). The conditions for the evolution $|\psi_n\rangle_s \to |\Upsilon_k\rangle_s$ to be a unitary transformation on system s are presented in Lapaire *et al.* [61]. If s describes the qubits and a the ancilla, they guarantee, as mentioned above, that the detection of $\hat{B}_k$ does not reveal any information about the qubits.

Especially, in the setup considered in this paper the system s consists of a set of N stationary qubits occupying a Hilbert space of size 2^N, and system a consists of N flying quantum systems occupying a Hilbert space of dimension $d \geqslant 2^N$. A measurement of the observable B on the flying qubits will result in a multiqubit (entangling) operation on the stationary qubits. We are interested in the case where the projector $\hat{B}_k$ induces a *unitary* transformation on the stationary qubits,

$$|\Upsilon_k\rangle_s = U_k|\Psi\rangle_s, \tag{4}$$

which means that $\hat{B}_k$ is a proper projector. There are two interesting cases to consider.

(1) The set $\{\hat{B}_k\}_a$ corresponds to a basis of states that induces a complete set $\{U_k\}_a$ of entangling quantum gates. As a result, finding any measurement outcome k will induce a unitary entangling gate operation on the stationary qubits.

(2) The set $\{\hat{B}_k\}_a$ corresponds to a basis that can be divided into two sets of states. Some of the projectors will induce a unitary entangling gate U_k on the stationary qubits, while the remaining projectors induce a transformation that is locally equivalent to the identity map $\mathbb{1}$.

The second setup is interesting for the following reason: Suppose that system s consists of N noninteracting (e.g., well-separated) stationary qubits with long decoherence times. If this system can generate flying qubits in the manner described above, we can perform a measurement of the observable B and entangle the noninteracting stationary qubits. When not all measurement outcomes produce an entangling gate on the stationary qubits (some yield instead the identity operator), then the unitary gate is applied only part of the time. However, due to the fact that a gate failure corresponds to an identity operation (or something locally equivalent), we can again prepare the flying qubits in the state $|A_0\rangle_a$. This allows us to repeat the protocol until the entangling gate is applied successfully, which is why we called this idea repeat-until-success quantum computing [43].

III. REMOTE TWO-QUBIT PHASE GATES

One of the requirements for universal quantum computing is the ability to perform an entangling two-qubit gate operation, like a controlled phase gate [62]. In this section we describe the general concept for the implementation of this

gate between two distant single photon sources. Note that our method of distributed quantum computing allows to realize entangling operations, since the measurement on a photon pair can imprint a phase on the state of its sources although it cannot change the distribution of their populations. The first step for the implementation of a two-qubit gate is the generation of a photon within each respective source, which encodes the information of the stationary qubit.

A. Encoding

Let us denote the states of the photon sources, which encode the logical qubits $|0\rangle_L$ and $|1\rangle_L$ as $|0\rangle$ and $|1\rangle$, respectively. An arbitrary pure state of two stationary qubits can then be written as

$$|\psi_{\text{in}}\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle, \tag{5}$$

where α, β, γ, and δ are complex coefficients with $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. Suppose that a photon is generated in each of the two sources, whose state (i.e., its polarization or generation time) depends on the state of the respective source. In the following we assume that source 1 prepared in $|i\rangle$ leads to the creation of one photon in state $|\mathsf{x}_i\rangle$, while source 2 prepared in $|i\rangle$ leads to the creation of one photon in state $|\mathsf{y}_i\rangle$,

$$|i\rangle_1 \to |i,\mathsf{x}_i\rangle_1, |i\rangle_2 \to |i,\mathsf{y}_i\rangle_2. \tag{6}$$

The simultaneous creation of a photon in both sources then transfers the initial state (5) into

$$|\psi_{\text{enc}}\rangle = \alpha|00,\mathsf{x}_0\mathsf{y}_0\rangle + \beta|01,\mathsf{x}_0\mathsf{y}_1\rangle + \gamma|10,\mathsf{x}_1\mathsf{y}_0\rangle + \delta|11,\mathsf{x}_1\mathsf{y}_1\rangle. \tag{7}$$

Note that the generation of photons whose state depends on the states of the stationary qubits is a highly nonlinear process. The preparation of the generally entangled state (7) is indeed the key step which allows the completion of an eventually deterministic two-qubit gate with otherwise nothing else than linear optics and photon pair measurements. The way the encoding step (6) can be realized experimentally is discussed in Sec. IV. In this section we focus on the general ideas underlying RUS quantum computing.

B. Mutually unbiased basis

Once the photons have been created, an entangling phase gate can be implemented by performing an absorbing measurement on the photon pair. Thereby, it is important to choose the photon measurement such that none of the possible outcomes reveals any information about the coefficients α, β, γ, and δ, as mentioned in Sec. II. This can be achieved with a photon pair measurement in a basis mutually unbiased [55] with respect to the computational basis given by the states $\{|\mathsf{x}_0\mathsf{y}_0\rangle, |\mathsf{x}_0\mathsf{y}_1\rangle, |\mathsf{x}_1\mathsf{y}_0\rangle, |\mathsf{x}_1\mathsf{y}_1\rangle\}$. More concretely, all possible outcomes of the photon measurement should be of the form

$$|\Phi\rangle = \tfrac{1}{2}[|\mathsf{x}_0\mathsf{y}_0\rangle + e^{i\varphi_1}|\mathsf{x}_0\mathsf{y}_1\rangle + e^{i\varphi_2}|\mathsf{x}_1\mathsf{y}_0\rangle + e^{i\varphi_3}|\mathsf{x}_1\mathsf{y}_1\rangle]. \tag{8}$$

As we see below, a complete set of basis states of this form can be found. Any bias in the amplitudes would yield information about α, β, γ, and δ, and would therefore not induce a unitary gate on the stationary qubits. Detecting the state (8) and absorbing the two photons in the process transfers the encoded state (7) into

$$|\psi_{\text{out}}\rangle = \alpha|00\rangle + e^{-i\varphi_1}\beta|01\rangle + e^{-i\varphi_2}\gamma|10\rangle + e^{-i\varphi_3}\delta|11\rangle. \tag{9}$$

Note that the output state (9) differs from the initial state (5) by a two-qubit phase gate.

Let us now consider the angle

$$\varphi_3 = \varphi_1 + \varphi_2. \tag{10}$$

In this case, the state $|\Phi\rangle$ is a product state and the output (9) differs from the initial state (5) only by local operations. However, if

$$\varphi_3 = \varphi_1 + \varphi_2 + \pi, \tag{11}$$

the state (8) becomes a maximally entangled state, as it becomes obvious when writing $|\Phi\rangle$ as

$$|\Phi\rangle = \tfrac{1}{2}[|\mathsf{x}_0\rangle(|\mathsf{y}_0\rangle + e^{i\varphi_1}|\mathsf{y}_1\rangle) + e^{i\varphi_2}|\mathsf{x}_1\rangle(|\mathsf{y}_0\rangle - e^{i\varphi_1}|\mathsf{y}_1\rangle)]. \tag{12}$$

The detection of a photon pair in this maximally entangled state results in the completion of a phase gate with maximum entangling power on the stationary qubits. Vice versa, maximum entanglement of the state (8) also automatically implies Eq. (11) as one can show by calculating the entanglement of formation of the state (8).

C. A deterministic gate

In the following, we denote the states of the measurement basis, i.e., the mutually unbiased basis, by $\{|\Phi_i\rangle\}$. In order to find a complete Bell basis with all states of form (8), we define

$$|\Phi_1\rangle \equiv \frac{1}{\sqrt{2}}[|\mathsf{a}_1\mathsf{b}_1\rangle + |\mathsf{a}_2\mathsf{b}_2\rangle],$$

$$|\Phi_2\rangle \equiv \frac{1}{\sqrt{2}}[|\mathsf{a}_1\mathsf{b}_1\rangle - |\mathsf{a}_2\mathsf{b}_2\rangle],$$

$$|\Phi_3\rangle \equiv \frac{1}{\sqrt{2}}[|\mathsf{a}_1\mathsf{b}_2\rangle + |\mathsf{a}_2\mathsf{b}_1\rangle],$$

$$|\Phi_4\rangle \equiv \frac{1}{\sqrt{2}}[|\mathsf{a}_1\mathsf{b}_2\rangle - |\mathsf{a}_2\mathsf{b}_1\rangle], \tag{13}$$

where the states $|\mathsf{a}_i\rangle$ describe photon 1 and the $|\mathsf{b}_i\rangle$ describe photon 2. Assuming orthogonality, i.e., $\langle\mathsf{a}_1|\mathsf{a}_2\rangle = 0$ and $\langle\mathsf{b}_1|\mathsf{b}_2\rangle = 0$, one can write the photon states on the right-hand side of Eq. (13) without loss of generality as

$$|\mathsf{a}_1\rangle = c_1|\mathsf{x}_0\rangle + e^{i\vartheta_1}s_1|\mathsf{x}_1\rangle,$$

$$|\mathsf{a}_2\rangle = e^{-i\xi_1}(e^{-i\vartheta_1}s_1|\mathsf{x}_0\rangle - c_1|\mathsf{x}_1\rangle),$$

$$|\mathsf{b}_1\rangle = c_2|\mathsf{y}_0\rangle + e^{i\vartheta_2}s_2|\mathsf{y}_1\rangle,$$

$$|\mathsf{b}_2\rangle = e^{-\mathrm{i}\xi_2}(e^{-\mathrm{i}\vartheta_2}s_2|\mathsf{y}_0\rangle - c_2|\mathsf{y}_1\rangle) \tag{14}$$

with

$$s_i \equiv \sin\theta_i,\ c_i \equiv \cos\theta_i. \tag{15}$$

Inserting this into Eq. (13), we find

$$\begin{aligned}|\Phi_1\rangle = \frac{1}{\sqrt{2}}[&(c_1c_2 + e^{-\mathrm{i}(\vartheta_1+\vartheta_2)}e^{-\mathrm{i}(\xi_1+\xi_2)}s_1s_2)|\mathsf{x}_0\mathsf{y}_0\rangle + (e^{\mathrm{i}\vartheta_2}c_1s_2\\ &- e^{-\mathrm{i}\vartheta_1}e^{-\mathrm{i}(\xi_1+\xi_2)}s_1c_2)|\mathsf{x}_0\mathsf{y}_1\rangle + (e^{\mathrm{i}\vartheta_1}s_1c_2\\ &- e^{-\mathrm{i}\vartheta_2}e^{-\mathrm{i}(\xi_1+\xi_2)}c_1s_2)|\mathsf{x}_1\mathsf{y}_0\rangle + (e^{\mathrm{i}(\vartheta_1+\vartheta_2)}s_1s_2\\ &+ e^{-\mathrm{i}(\xi_1+\xi_2)}c_1c_2)|\mathsf{x}_1\mathsf{y}_1\rangle],\end{aligned}$$

$$\begin{aligned}|\Phi_2\rangle = \frac{1}{\sqrt{2}}[&(c_1c_2 - e^{-\mathrm{i}(\vartheta_1+\vartheta_2)}e^{-\mathrm{i}(\xi_1+\xi_2)}s_1s_2)|\mathsf{x}_0\mathsf{y}_0\rangle + (e^{\mathrm{i}\vartheta_2}c_1s_2\\ &+ e^{-\mathrm{i}\vartheta_1}e^{-\mathrm{i}(\xi_1+\xi_2)}s_1c_2)|\mathsf{x}_0\mathsf{y}_1\rangle + (e^{\mathrm{i}\vartheta_1}s_1c_2\\ &+ e^{-\mathrm{i}\vartheta_2}e^{-\mathrm{i}(\xi_1+\xi_2)}c_1s_2)|\mathsf{x}_1\mathsf{y}_0\rangle + (e^{\mathrm{i}(\vartheta_1+\vartheta_2)}s_1s_2\\ &- e^{-\mathrm{i}(\xi_1+\xi_2)}c_1c_2)|\mathsf{x}_1\mathsf{y}_1\rangle],\end{aligned}$$

$$\begin{aligned}|\Phi_3\rangle = \frac{1}{\sqrt{2}}[&(e^{-\mathrm{i}\vartheta_2}e^{-\mathrm{i}\xi_2}c_1s_2 + e^{-\mathrm{i}\vartheta_1}e^{-\mathrm{i}\xi_1}s_1c_2)|\mathsf{x}_0\mathsf{y}_0\rangle - (e^{-\mathrm{i}\xi_2}c_1c_2\\ &- e^{-\mathrm{i}(\vartheta_1-\vartheta_2)}e^{-\mathrm{i}\xi_1}s_1s_2)|\mathsf{x}_0\mathsf{y}_1\rangle + (e^{\mathrm{i}(\vartheta_1-\vartheta_2)}e^{-\mathrm{i}\xi_2}s_1s_2\\ &- e^{-\mathrm{i}\xi_1}c_1c_2)|\mathsf{x}_1\mathsf{y}_0\rangle - (e^{\mathrm{i}\vartheta_1}e^{-\mathrm{i}\xi_2}s_1c_2 + e^{\mathrm{i}\vartheta_2}e^{-\mathrm{i}\xi_1}c_1s_2)\\ &\times|\mathsf{x}_1\mathsf{y}_1\rangle],\end{aligned}$$

$$\begin{aligned}|\Phi_4\rangle = \frac{1}{\sqrt{2}}[&(e^{-\mathrm{i}\vartheta_2}e^{-\mathrm{i}\xi_2}c_1s_2 - e^{-\mathrm{i}\vartheta_1}e^{-\mathrm{i}\xi_1}s_1c_2)|\mathsf{x}_0\mathsf{y}_0\rangle - (e^{-\mathrm{i}\xi_2}c_1c_2\\ &+ e^{-\mathrm{i}(\vartheta_1-\vartheta_2)}e^{-\mathrm{i}\xi_1}s_1s_2)|\mathsf{x}_0\mathsf{y}_1\rangle + (e^{\mathrm{i}(\vartheta_1-\vartheta_2)}e^{-\mathrm{i}\xi_2}s_1s_2\\ &+ e^{-\mathrm{i}\xi_1}c_1c_2)|\mathsf{x}_1\mathsf{y}_0\rangle - (e^{\mathrm{i}\vartheta_1}e^{-\mathrm{i}\xi_2}s_1c_2 - e^{\mathrm{i}\vartheta_2}e^{-\mathrm{i}\xi_1}c_1s_2)\\ &\times|\mathsf{x}_1\mathsf{y}_1\rangle].\end{aligned} \tag{16}$$

These states are of the form (8), if the amplitudes are all of the same size, which yields the conditions

$$|c_1c_2 \pm e^{-\mathrm{i}(\vartheta_1+\vartheta_2+\xi_1+\xi_2)}s_1s_2| = |c_1s_2 \pm e^{-\mathrm{i}(\vartheta_1+\vartheta_2+\xi_1+\xi_2)}s_1c_2| = \frac{1}{\sqrt{2}}, \tag{17}$$

and

$$|c_1s_2 \pm e^{-\mathrm{i}(\vartheta_1-\vartheta_2+\xi_1-\xi_2)}s_1c_2| = |c_1c_2 \pm e^{-\mathrm{i}(\vartheta_1-\vartheta_2+\xi_1-\xi_2)}s_1s_2| = \frac{1}{\sqrt{2}}. \tag{18}$$

The only solution of the constraints (17) and (18) is

$$\cos(2\theta_1)\cos(2\theta_2) = \cos(\vartheta_1 \pm \vartheta_2 + \xi_1 \pm \xi_2) = 0 \tag{19}$$

provided that neither $\cos(2\theta_1)$ nor $\cos(2\theta_2)$ equals 1. In the special case, where either $\cos(2\theta_1)=1$ or $\cos(2\theta_2)=1$, condition (19) simplifies to $\cos(2\theta_1)\cos(2\theta_2)=0$ with no restrictions in the angles ϑ_1, ϑ_2, ξ_1, and ξ_2.

One particular way to fulfill the restrictions (19) is to set

$$\xi_2 = -\tfrac{1}{2}\pi,\quad \xi_1 = \vartheta_1 = \vartheta_2 = 0, \text{ and } \theta_1 = \theta_2 = \tfrac{1}{4}\pi, \tag{20}$$

which corresponds to the choice (cf. [43])

$$\begin{aligned}|\mathsf{a}_1\rangle &= \frac{1}{\sqrt{2}}(|\mathsf{x}_0\rangle + |\mathsf{x}_1\rangle),\\ |\mathsf{a}_2\rangle &= \frac{1}{\sqrt{2}}(|\mathsf{x}_0\rangle - |\mathsf{x}_1\rangle),\\ |\mathsf{b}_1\rangle &= \frac{1}{\sqrt{2}}(|\mathsf{y}_0\rangle + |\mathsf{y}_1\rangle),\\ |\mathsf{b}_2\rangle &= \frac{\mathrm{i}}{\sqrt{2}}(|\mathsf{y}_0\rangle - |\mathsf{y}_1\rangle),\end{aligned} \tag{21}$$

and yields

$$\begin{aligned}|\Phi_1\rangle &= \tfrac{1}{2}e^{\mathrm{i}\pi/4}[|\mathsf{x}_0\mathsf{y}_0\rangle - i|\mathsf{x}_0\mathsf{y}_1\rangle - i|\mathsf{x}_1\mathsf{y}_0\rangle + |\mathsf{x}_1\mathsf{y}_1\rangle],\\ |\Phi_2\rangle &= \tfrac{1}{2}e^{-\mathrm{i}\pi/4}[|\mathsf{x}_0\mathsf{y}_0\rangle + i|\mathsf{x}_0\mathsf{y}_1\rangle + i|\mathsf{x}_1\mathsf{y}_0\rangle + |\mathsf{x}_1\mathsf{y}_1\rangle],\\ |\Phi_3\rangle &= \tfrac{1}{2}e^{\mathrm{i}\pi/4}[|\mathsf{x}_0\mathsf{y}_0\rangle - i|\mathsf{x}_0\mathsf{y}_1\rangle + i|\mathsf{x}_1\mathsf{y}_0\rangle - |\mathsf{x}_1\mathsf{y}_1\rangle],\\ |\Phi_4\rangle &= -\tfrac{1}{2}e^{-i\pi/4}[|\mathsf{x}_0\mathsf{y}_0\rangle + i|\mathsf{x}_0\mathsf{y}_1\rangle - i|\mathsf{x}_1\mathsf{y}_0\rangle - |\mathsf{x}_1\mathsf{y}_1\rangle].\end{aligned} \tag{22}$$

To find out which gate operation the detection of the corresponding maximally entangled states (13) combined with a subsequent absorption of the photon pair results into, we write the input state (7) as

$$|\psi_{\mathrm{enc}}\rangle = \tfrac{1}{2}\sum_i^4 |\psi_i\rangle \otimes |\Phi_i\rangle \tag{23}$$

and determine the states $|\psi_i\rangle$ of the stationary qubits. Using the notation

$$U_{\mathrm{CZ}} \equiv |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11| \tag{24}$$

for the controlled two-qubit phase gate [the controlled-Z (CZ) gate] and the notation

$$Z_i(\phi) \equiv |0\rangle_{\mathrm{ii}}\langle 0| + e^{-\mathrm{i}\phi}|1\rangle_{\mathrm{ii}}\langle 1| \tag{25}$$

for the local controlled-Z gate on photon source i [63], we find

$$\begin{aligned}|\psi_1\rangle &= \exp\left(-\tfrac{1}{4}i\pi\right)Z_2\left(-\tfrac{1}{2}\pi\right)Z_1\left(-\tfrac{1}{2}\pi\right)U_{\mathrm{CZ}}|\psi_{\mathrm{in}}\rangle,\\ |\psi_2\rangle &= \exp\left(\tfrac{1}{4}i\pi\right)Z_2\left(\tfrac{1}{2}\pi\right)Z_1\left(\tfrac{1}{2}\pi\right)U_{\mathrm{CZ}}|\psi_{\mathrm{in}}\rangle,\\ |\psi_3\rangle &= \exp\left(-\tfrac{1}{4}i\pi\right)Z_2\left(-\tfrac{1}{2}\pi\right)Z_1\left(\tfrac{1}{2}\pi\right)U_{\mathrm{CZ}}|\psi_{\mathrm{in}}\rangle,\\ |\psi_4\rangle &= -\exp\left(\tfrac{1}{4}i\pi\right)Z_2\left(\tfrac{1}{2}\pi\right)Z_1\left(-\tfrac{1}{2}\pi\right)U_{\mathrm{CZ}}|\psi_{\mathrm{in}}\rangle.\end{aligned} \tag{26}$$

From this we see that one can indeed obtain the CZ gate operation (24) up to local unitary operations upon the detection of any of the four Bell states $|\Phi_i\rangle$, as it has been pointed out already by Protsenko *et al.* [42].

D. Repeat-until-success quantum computing

When implementing distributed quantum computing with photons as flying qubits, the problem arises that it is impossible to perform a complete deterministic Bell measurement on the photons using only linear optics elements. As it has been shown [64], in the best case, one can distinguish two of the four Bell states. Since the construction of efficient nonlinear optical elements remains experimentally challenging, the above described phase gate could therefore be operated at most with a success rate of 1/2.

What must be done to solve this problem is to choose the photon pair measurement basis $\{|\Phi_i\rangle\}$ such that two of the basis states are maximally entangled while the other two basis states are product states. Most importantly, all basis states must be mutually unbiased with respect to the computational basis and information will not be destroyed at any stage of the computation. In the following we choose $|\Phi_3\rangle$ and $|\Phi_4\rangle$ as in Eq. (13) and $|\Phi_1\rangle$ and $|\Phi_2\rangle$ as product states such that

$$|\Phi_1\rangle = |\mathsf{a}_1\mathsf{b}_1\rangle, \quad |\Phi_2\rangle = |\mathsf{a}_2\mathsf{b}_2\rangle,$$

$$|\Phi_3\rangle \equiv \frac{1}{\sqrt{2}}[|\mathsf{a}_1\mathsf{b}_2\rangle + |\mathsf{a}_2\mathsf{b}_1\rangle],$$

$$|\Phi_4\rangle \equiv \frac{1}{\sqrt{2}}[|\mathsf{a}_1\mathsf{b}_2\rangle - |\mathsf{a}_2\mathsf{b}_1\rangle]. \tag{27}$$

The aim of this is (see Sec. II) that in the event of the "failure" of the gate implementation (i.e., in case of the detection of $|\Phi_1\rangle$ or $|\Phi_2\rangle$) the system remains, up to a local phase gate, in the original qubit state. This means that the initial state (5) can be restored and the described protocol can be repeated, thereby eventually resulting in the performance of the universal controlled phase gate (24). The probability for the realization of the gate operation within one step equals 1/2 and the final completion of a quantum phase gate therefore requires on average *two* repetitions of the above described photon pair generation and detection process.

Let us now determine the conditions under which the states $\{|\Phi_i\rangle\}$ are of the form (8). Proceeding as above, we find that the angles ϑ_i, ξ_i, and θ_i in Eq. (14) should fulfill, for example, Eq. (20). In analogy to Eqs. (17) and (18), we find that $|\Phi_1\rangle$ and $|\Phi_2\rangle$ are mutually unbiased if

$$|c_1c_2| = |c_1s_2| = |s_1c_2| = |s_1s_2| = \tfrac{1}{2}, \tag{28}$$

which also holds for the parameter choice in Eq. (20). Using Eq. (21), one can easily verify that with the above choice the basis (27) becomes

$$|\Phi_1\rangle = \tfrac{1}{2}[|\mathsf{x}_0\mathsf{y}_0\rangle + |\mathsf{x}_0\mathsf{y}_1\rangle + |\mathsf{x}_1\mathsf{y}_0\rangle + |\mathsf{x}_1\mathsf{y}_1\rangle],$$

$$|\Phi_2\rangle = \frac{i}{2}[|\mathsf{x}_0\mathsf{y}_0\rangle - |\mathsf{x}_0\mathsf{y}_1\rangle - |\mathsf{x}_1\mathsf{y}_0\rangle + |\mathsf{x}_1\mathsf{y}_1\rangle],$$

$$|\Phi_3\rangle = \tfrac{1}{2}e^{i\pi/4}[|\mathsf{x}_0\mathsf{y}_0\rangle - i|\mathsf{x}_0\mathsf{y}_1\rangle + i|\mathsf{x}_1\mathsf{y}_0\rangle - |\mathsf{x}_1\mathsf{y}_1\rangle],$$

$$|\Phi_4\rangle = -\tfrac{1}{2}e^{-i\pi/4}[|\mathsf{x}_0\mathsf{y}_0\rangle + i|\mathsf{x}_0\mathsf{y}_1\rangle - i|\mathsf{x}_1\mathsf{y}_0\rangle - |\mathsf{x}_1\mathsf{y}_1\rangle]. \tag{29}$$

Choosing the states $|\mathsf{a}_i\rangle$ and $|\mathsf{b}_i\rangle$ as in Eq. (21) allows to implement the gate operation (24) eventually deterministically.

Finally, we determine the gate operations corresponding to the detection of a certain measurement outcome $|\Phi_i\rangle$. To do this, we decompose the input state (7) again into a state of the form (23). Proceeding as in the previous section, we find

$$|\psi_1\rangle = |\psi_{\text{in}}\rangle,$$

$$|\psi_2\rangle = -iZ_2(\pi)Z_2(\pi)|\psi_{\text{in}}\rangle,$$

$$|\psi_3\rangle = \exp\left(-\tfrac{1}{4}i\pi\right)Z_2\left(-\tfrac{1}{2}\pi\right)Z_1\left(\tfrac{1}{2}\pi\right)U_{\text{CZ}}|\psi_{\text{in}}\rangle,$$

$$|\psi_4\rangle = -\exp\left(\tfrac{1}{4}i\pi\right)Z_2\left(\tfrac{1}{2}\pi\right)Z_1\left(-\tfrac{1}{2}\pi\right)U_{\text{CZ}}|\psi_{\text{in}}\rangle. \tag{30}$$

Again one obtains the CZ gate operation (24) up to local unitary operations upon the detection of either $|\Phi_3\rangle$ or $|\Phi_4\rangle$. In the event of the detection of the product states $|\Phi_1\rangle$ or $|\Phi_2\rangle$, the initial state can be restored with the help of one-qubit phase gates, which then allows us to repeat the operation until success.

It should be emphasized that there are other possible encodings that yield a universal two-qubit phase gate upon the detection of a Bell-state, but where the original state is destroyed upon the detection of a product state (see, e.g., [40]). This happens when the product states are not mutually unbiased and their detection erases the qubit states in the respective photon sources. To achieve the effect of an *insurance* against failure, the encoding (6) should be chosen as described in this section.

IV. POSSIBLE EXPERIMENTAL REALIZATIONS

Possible experimental realizations of the above described eventually deterministic quantum phase gate consist of two basic steps. Firstly, the information of the stationary qubits involved in the operation has to be redundantly encoded in the states of two newly generated ancilla photons. Afterwards, a measurement is performed on the photon pair resulting with probability 1/2 in the desired gate operation. Depending on the type of photon source, one can choose different types of encoding. There are also different possibilities how to perform the photon pair measurement. Examples are given below.

A. Redundant encoding

In order to obtain robust qubits, the states $|0\rangle$ and $|1\rangle$ should be two different long-living ground states of the single photon source. Each photon source carries one qubit. Depending on its level structure (see Fig. 3), it might be advantageous to realize the encoding step (7) either by generating photons with different polarizations (polarization encoding) or photons that agree in all degrees of freedom apart from their creation time (time bin encoding). Note that dif-

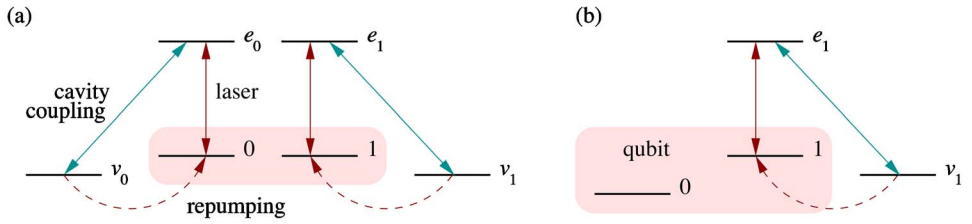

FIG. 3. (Color online) Schematic view of a single photon (a) polarization encoder, (b) time-bin encoder, and level configuration of the source containing the qubit.

ferent encodings can easily be transformed into each other using linear optics elements like a polarizing beam splitters and delaying photons in time.

Polarization encoding. Suppose, the photon source contains an atomic double Λ level configuration as shown in Fig. 3(a) (see also Ref. [65]). A single photon can then be created by simultaneously applying a laser pulse with increasing Rabi frequency to the 0-e_0 transition and the 1-e_1 transition of the atomic system. Thereby, the atom goes to the ground state $|v_0\rangle$ and $|v_1\rangle$, respectively, depending on whether its initial state equalled $|0\rangle$ or $|1\rangle$ due to the coupling of the e_0-v_0 transition and the e_1-v_1 transition to the cavity mode. It has been shown in the past that this technique [66] is very well suited to place exactly one excitation into the field of an optical resonator, from where it can leak out [47].

If the two transitions, e_0-v_0 and e_1-v_1, couple to the two different polarization modes h and v, in the cavity field, the photon generation results effectively, for example, in the operation

$$|0\rangle_i \to |0,\mathsf{h}\rangle_i, \quad |1\rangle_i \to |1,\mathsf{v}\rangle_i \tag{31}$$

once atom i has been repumped into its initial state $|0\rangle_i$ and $|1\rangle_i$, respectively. Finally we remark that the encoding does not affect the coefficients α, β, γ, and δ of the initial state (5). As long as no measurement is performed on the system all coherences are preserved.

Time-bin encoding. Alternatively, if the photon sources possess a level structure like the one shown in Figure 3(b), one can redundantly encode the information contained in the qubits into time bin encoded photons,

$$|0\rangle_i \to |0,\mathsf{E}\rangle_i, \quad |1\rangle_i \to |1,\mathsf{L}\rangle_i. \tag{32}$$

This encoding is simpler and may therefore find realizations not only in atoms but also in quantum dots and nitrogen vacancy color centers. In Eq. (32), $|\mathsf{E}\rangle$ and $|\mathsf{L}\rangle$ denote a single photon generated at an *early* and a *later* time, respectively. The above operation can be achieved by first coupling a laser field with increasing Rabi frequency to the 1-e_1 transition, while the cavity mode couples to the e_1-v_1 transition. Once the excitation has been placed into the cavity mode and leaked out through the outcoupling mirror, the atom can be repumped into $|0\rangle$. Afterwards, one should swap the states $|0\rangle$ and $|1\rangle$ and repeat the process. This results in the generation of a late photon, if the system was initially prepared in $|1\rangle$. To complete the encoding, the states $|0\rangle$ and $|1\rangle$ have to be swapped again.

B. Photon pair measurement

We now give two examples how to perform a photon pair measurement of the mutually unbiased basis (29). The first method is suitable for polarization encoded photons, the second one for dual rail encoded photons. If the qubits have initially been time bin encoded, their encoding should be transformed first using standard linear optics techniques.

Polarization encoding. It is well known that sending two polarization encoded photons through the different input ports of a 50:50 beam splitter together with polarization sensitive measurements in the $|\mathsf{h}\rangle/|\mathsf{v}\rangle$ basis in the output ports would result in a measurement of the states $1/(\sqrt{2})\times(|\mathsf{hv}\rangle \pm |\mathsf{vh}\rangle)$, $|\mathsf{hh}\rangle$ and $|\mathsf{vv}\rangle$. To measure the states (27), we therefore propose to proceed as shown in Fig. 4(a) [43] and to perform the mapping

$$U_1 = |\mathsf{h}\rangle\langle \mathsf{a}_1| + |\mathsf{v}\rangle\langle \mathsf{a}_2|,$$

$$U_2 = |\mathsf{h}\rangle\langle \mathsf{b}_1| + |\mathsf{v}\rangle\langle \mathsf{b}_2| \tag{33}$$

on the photon coming from source i. Using Eq. (21), we see that this corresponds to the single qubit rotations

$$U_1 = \frac{1}{\sqrt{2}}[|\mathsf{h}\rangle(\langle \mathsf{h}| + \langle \mathsf{v}|) + |\mathsf{v}\rangle(\langle \mathsf{h}| - \langle \mathsf{v}|)],$$

$$U_2 = \frac{1}{\sqrt{2}}[|\mathsf{h}\rangle(\langle \mathsf{h}| + \langle \mathsf{v}|) - i|\mathsf{v}\rangle(\langle \mathsf{h}| - \langle \mathsf{v}|)]. \tag{34}$$

After leaving the beam splitter, the photons should be detected in the $|\mathsf{h}\rangle/|\mathsf{v}\rangle$ basis. A detection of two h and two v polarized photons indicates a measurement of $|\Phi_1\rangle$ and $|\Phi_2\rangle$, respectively. Finding two photons of different polarization in the same or in different detectors corresponds to a detection of $|\Phi_3\rangle$ or $|\Phi_4\rangle$.

Dual-rail encoding. Alternatively, one can redirect the generated photons to the different input ports of a 4×4 Bell

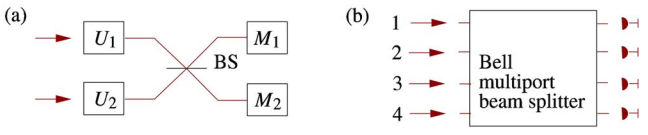

FIG. 4. (Color online) Linear optics networks for the realization of a measurement of the basis states (13) after encoding the photonic qubits in the polarization degrees of two photons (a) or into four different spatial photon modes (b) involving either a beam splitter or a 4×4 Bell multiport beam splitter.

multiport beam splitter as shown in Fig. 4(b). If $a_n^\dagger$ and $b_n^\dagger$ denotes the creation operator for a photon in input and output port n, respectively, the effect of the multiport can be summarized as [67]

$$a_n^\dagger \rightarrow \sum_m U_{mn} b_m^\dagger \tag{35}$$

with

$$U_{mn} = \tfrac{1}{2} \exp[i\pi(n-1)(m-1)]. \tag{36}$$

A Bell multiport redirects each incoming photon with equal probability to any of the possible output ports, thereby erasing the which way information of the incoming photons. One way to measure in the mutually unbiased basis (29) is to direct the $|\mathsf{x}_0\rangle$ photon from source 1 to input port 1, the $|\mathsf{x}_1\rangle$ photon from source 1 to input port 3, and to direct the $|\mathsf{y}_0\rangle$ photon and the $|\mathsf{y}_1\rangle$ photon from source 2 to input port 2 and 4, respectively. If $|\text{vac}\rangle$ denotes the state with no photons in the setup, this results in the conversion

$$|\mathsf{x}_0\mathsf{y}_0\rangle \rightarrow a_1^\dagger a_2^\dagger|\text{vac}\rangle, \quad |\mathsf{x}_0\mathsf{y}_1\rangle \rightarrow a_1^\dagger a_4^\dagger|\text{vac}\rangle,$$

$$|\mathsf{x}_1\mathsf{y}_0\rangle \rightarrow a_2^\dagger a_3^\dagger|\text{vac}\rangle, \quad |\mathsf{x}_1\mathsf{y}_1\rangle \rightarrow a_3^\dagger a_4^\dagger|\text{vac}\rangle. \tag{37}$$

This conversion should be realized such that the photons enter the multiport at the same time. Using Eq. (35) one can show that the network transfers the basis states (29) according to

$$|\Phi_1\rangle \rightarrow \tfrac{1}{2}(b_1^{\dagger 2} - b_3^{\dagger 2})|\text{vac}\rangle,$$

$$|\Phi_2\rangle \rightarrow -\tfrac{1}{2}(b_2^{\dagger 2} - b_4^{\dagger 2})|\text{vac}\rangle,$$

$$|\Phi_3\rangle \rightarrow \frac{1}{\sqrt{2}}(b_1^\dagger b_4^\dagger - b_2^\dagger b_3^\dagger)|\text{vac}\rangle,$$

$$|\Phi_4\rangle \rightarrow -\frac{1}{\sqrt{2}}(b_1^\dagger b_2^\dagger - b_3^\dagger b_4^\dagger)|\text{vac}\rangle. \tag{38}$$

Finally, detectors measure the presence of photons in each of the possible output ports. The detection of two photons in the same output port, namely in 1 or 3 and in 2 or 4, corresponds to a measurement of the state $|\Phi_1\rangle$ and $|\Phi_2\rangle$, respectively. The detection of a photon in ports 1 and 4 or in 2 and 3 indicates a measurement of the state $|\Phi_3\rangle$, while a photon in the ports 1 and 2 or in 3 and 4 indicates the state $|\Phi_4\rangle$.

Any unknown fixed (or slowly varying with respect to the coherence length of the photon pulse) phase factor introduced along the photon paths contributes at most to a global phase factor to the input state (7), which is also a feature of the schemes outlined in Refs. [36,38,39,43]. The implementation of repeat-until-success quantum computing therefore does not require interferometric stability. It requires only overlapping of the photons within their coherence length within the linear optics setup.

V. SCALABLE QUANTUM COMPUTATION IN THE PRESENCE OF INEFFICIENT PHOTON GENERATION AND DETECTION

In this section, we discuss the possibility of implementing scalable quantum computation using the repeat-until-success quantum gate described in the previous sections. The implementation of this gate requires the generation of single photons on demand and linear optical elements together with absorbing quantum measurements. In the limit of perfect photon emission, collection, and detection efficiency, two-qubit CZ gates can be performed deterministically, as described above. In real systems, however, photon emission, collection, and detection is not perfect [68]. In existing experiments, all of these processes have significant inefficiencies, which means that there is a finite probability that two photons will not be observed in the photon measurement. The failure to observe two photons in an attempted CZ operation means that the static qubits are left in an unknown state, which constitutes a correlated two-qubit error. If such losses are sufficiently small (e.g., less than $\sim 10^{-2}$), the resulting gate failures can be dealt with using existing fault tolerance techniques [69,70]. Recently, much higher fault tolerance levels of up to 50% were found in linear optical quantum computing [71,72].

More concretely, the highest reported photon detection efficiency for single photon detection with photon number resolution is about 88% [53,73]. A recent experiment by McKeever *et al.* [49] involving an atom cavity system for the generation of single photons on demand yields a photon generation efficiency of nearly 70%, limited only by passive cavity loss. The lifetime of the atom in the cavity was 0.14 s, allowing for as many as 1.4×10^4 photon generation events. Moreover, Legero *et al.* [74] demonstrated perfect time resolved interference with two photons of different frequencies. Time resolved detection acts as a temporal filter to erase the which way information that is important to any scheme involving photon interference. This suggests that strictly identical single photon sources are not required for attaining high fidelities in the state preparation. The cost of this high fidelity is a lower probability of success.

Fortunately, scalable quantum computing is possible, even in the presence of large errors, as long as no errors imply a very high fidelity and the occurrence of an error is *heralded*. If fewer than two photons are detected, we know that the attempted CZ operation has failed. Only when the detectors have a substantial amount of dark counts, we cannot rely on this error detection mechanism. However, commercially available silicon avalanche photodetectors are available with a detection efficiency of 65%, and a dark count rate of $\Gamma_{dc} \leqslant 25\ \text{s}^{-1}$ [75]. A photon regeneration rate of 105 s^{-1} gives a clock time of 10^{-5} s. The total dark count probability is then $p_{dc} \approx 10^{-4}$ per clock cycle, which is small enough to be dealt with using existing error correction techniques. Moreover, if one could experiment with detectors like the one reported by Rosenberg *et al.* [53], dark count rate effects would be negligible.

In the case of an error, the state of the static qubits can be determined by subsequently performing measurements on the sources, which allows the sources to be reprepared in a

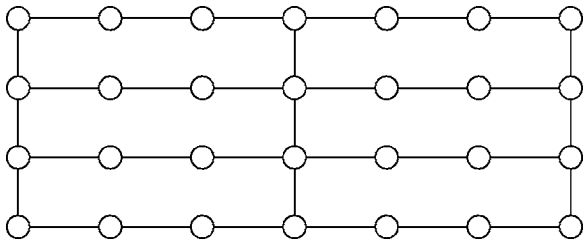

FIG. 5. A rectangular lattice cluster state. Each circle represents a physical qubit, and each line represents a bond between qubits. These states are sufficient for simulating arbitrary logic networks [15], with each horizontal row representing a single logical qubit, and each vertical connection representing a two-qubit gate. Note we also permit bonds between nonadjacent rows and columns (not shown), which can simulate non-nearest-neighbor two-qubit operations.

known state. In earlier work, we have shown that scalable quantum computation can be performed in the presence of significant heralded error rates, by first using a nondeterministic entangling operation to create *cluster states* of many qubits [44], and subsequently implementing scalable quantum computation via the "one-way quantum computer" [13]. Given cluster states of many qubits, the one-way quantum computer can be implemented by single qubit measurements alone. This technique permits fully scalable quantum computation, albeit with a fixed overhead per two-qubit gate in the algorithm, which we calculate below. We briefly review how one-way quantum computing can proceed within our scheme, and then provide an estimate of the overhead costs involved.

A. One-way quantum computation

One-way quantum computation [13] proceeds by first creating a graph state of many qubits, and subsequently performing single qubit measurements on the graph state [76–78]. Graph states may be represented as a graph comprising set of qubit "nodes" connected by "edges" which may be understood as "bonds" between the qubits. The quantum state corresponding to such a graph may be defined (and also implemented) by the following procedure: (i) prepare each qubit in the state $|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$, and then (ii) for each bond in the corresponding graph, apply a deterministic CZ operation [see Eq. (24)] between the relevant qubits. In this work, we will restrict our attention to the rectangular lattice graph states of the form shown in Fig. 5 (hereafter referred to simply as *cluster states*), which are sufficient for simulating arbitrary logic networks, and hence universal quantum computations [15]. It is worth noting, however, that straightforward generalizations of the procedure described below allow us to scalably generate *arbitrary* graph states. This may be useful in that it might result in reduced costs for implementing certain algorithms.

In these clusters, each horizontal row of physical qubits represents a single logical qubit in the logic network being simulated. Two qubit operations are implemented by the vertical bonds acting between rows. We also permit bonds between nonadjacent rows, which permits highly nonlocal two qubit gates to be implemented. Note also that the location of the qubits within the cluster is notional, and need not correspond to the physical location of the static qubit (the mapping between the notional qubit positions within the cluster and the actual physical location of the qubits can be stored in a classical computer). After making the state, quantum computation proceeds by performing a sequence of single qubit measurements on the static qubits, with each measurement performed in a particular basis so as to implement a given sequence of one- and two-qubit gates [13,15]. At each time step, a whole column of physical qubits in the cluster is measured. The measurements are performed in order, starting with the column at the left side of the cluster, and proceeding rightwards across the cluster. In general, the basis of the measurements made at a given time step will depend on the outcomes of earlier measurements. Once a physical qubit has been measured, that qubit is disentangled from the cluster state and so may be reinitialized in a particular state and subsequently used later in the computation.

We assume that single-shot single qubit measurements and single qubit unitary operations on the static qubits can be implemented using standard techniques. Implementing one-way quantum computation in our scheme therefore reduces to the problem of scalably generating cluster states using the heralded, nondeterministic CZ operation. We outline the general procedure here, and give a more detailed description in the subsequent section.

In our scheme, cluster states can be generated by attempting to bond qubits using the nondeterministic CZ operation. This operation has three possible outcomes: "success," "insurance," or "failure." In the case of observing two photons, one of the gates of Eq. (30) is implemented, and subsequent application of appropriate single qubit unitaries implements either the CZ operation (denoting a success), or the identity operation (denoting insurance). In the case of insurance, the CZ operation can simply be reattempted. Observing fewer than two photons denotes a failure. In this case, the static qubits are left in an unknown state. However, this damage can be repaired as follows. Firstly, each of the two qubits involved in the failed gate can be measured in the computational basis to determine the nature of the error. If either qubit was already part of a cluster state, the bonds to its neighbors within the cluster are also destroyed. However, the remainder of the cluster state can be recovered by applying appropriate single qubit unitary operations to these neighboring qubits, conditional on the outcome of the measurement on the qubit involved in the failed CZ gate. Therefore, the cluster state can grow, shrink, or remain the same size, depending on whether the CZ operation was successful, failed, or failed with insurance. The key to scalably generating cluster states is to attempt CZ operations between qubits in a sequence order such that the cluster state grows on average. We give such a sequence in Sec. V B.

We conclude this section by noting that it is not necessary to build the whole cluster required for simulating a particular algorithm before commencing the single qubit measurement part of the computation. It is possible to build a partial cluster, and then to simultaneously perform single qubit measurements on one part of the cluster, while adding new qubits to another region in the cluster. In this approach to one-way

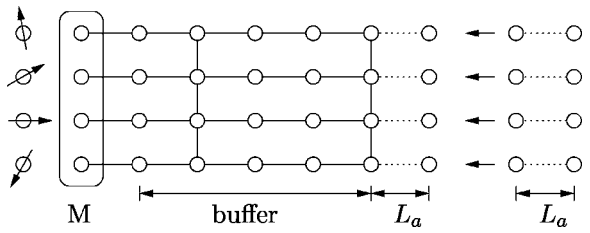

FIG. 6. Dynamically growing clusters during a computation. The cluster contains three regions: the active region (M) at the left of the cluster, in which the logic gate networks are being simulated via single qubit measurements; the buffer region; and the connection region, where new cluster fragments are added to the right edge of the main cluster. The connecting cluster chains have a buffer length L_a to accommodate the probabilistic entangling operation.

quantum computing, one can think of the cluster as being split into three regions, as shown in Fig. 6. The *active region*, to the left of the cluster, contains the part of the cluster where the logic gate networks are being simulated via single qubit measurements. At the right of the cluster, the *connection region* comprises of several horizontal dangling linear chains which extend from the right edge of the main cluster, each corresponding to a logical qubit. In this region, nondeterministic CZ operations are applied in order to add further cluster sections to the main section. These additional sections are manufactured separately, as described in Sec. V B. Between the active region and the connection region, the *buffer region* comprises a quiescent region which suffices to protect the active region in the event of a long sequence of failed CZ operations; this would lead to the right edge of the cluster running back into the active region, damaging the logical computation. The depth of the buffer region should be chosen such that the probability of erasing a logical qubit is sufficiently small that it can be handled with existing fault tolerance techniques [69,70].

There are several advantages to this approach. Firstly, fewer physical qubits are needed, because qubits that have already been measured at the left edge of the cluster can be recycled and added to the right hand side of the cluster. Secondly, preparing the whole cluster initially means that some of the qubits will spend a lot of time in an "idle" state before they are involved in the computation; any errors accumulated in these idle qubits due to decoherence will degrade the fidelity of the computation [13]. This is crucial if fault tolerant quantum computation is to be implemented within the cluster model, as such schemes require a source of fresh ancilla qubits throughout the algorithm. Thirdly, the overhead costs for this approach can be reduced, because it is not necessary to prepare the *whole* cluster with a total success probability close to one; the probability for erasing a given logical qubit need only be made smaller than the error threshold required for fault tolerance.

B. Overhead costs

A number of authors have considered efficient cluster state generation using nondeterministic, but heralded, entangling operations (EOs) [14–16,44,79–82]. References [14–16] calculated explicit costs for making cluster states of optical qubits in the ideal case (i.e., neglecting photon loss). Subsequently, Barrett and Kok [44] showed that, in the case of hybrid matter optical systems (such as those considered in this work), arbitrarily small EO success probabilities could be tolerated. They provided a "divide and conquer" algorithm for building linear clusters, which has moderate costs even for small success probability. An efficient algorithm for building two-dimensional clusters, capable of simulating arbitrary logic networks was also given in [44]. More recently, in Ref. [79], a similar algorithm for building linear clusters was proposed, which made more use of recycling, and hence has a lower overhead cost. Reference [79] also gives an alternative algorithm for making two-dimensional clusters, and explicitly calculates the associated overhead costs. In Ref. [80], some elegant cost reducing improvements to the scheme proposed in Ref. [44] were suggested, utilizing the redundantly encoded qubits inherent in the original scheme.

In this work, we will combine elements of the approaches taken in Refs. [16,44,79] to provide a simple upper bound for the scaling costs for building cluster states using our scheme. This estimate is based on an explicit procedure, and we do not claim that it is optimal; an improved algorithm may yield substantially reduced costs. Nevertheless, the procedure given here allows a straightforward calculation of the overhead costs. Despite its apparent similarity to Refs. [44,79], there is a crucial difference; in the scheme under consideration in this paper, there is the possibility of obtaining the insurance outcome. In general, this leads to a reduction in costs relative to schemes in which there is no insurance outcome.

In the presence of imperfect photon emission, detection, and collection, the performance of the CZ operation can be characterized by three probabilities.

(a) The probability of successfully implementing the CZ operation on the input qubits (up to local operations), p_s.

(b) The probability of obtaining the insurance outcome in which known local operations are applied to the qubits, p_i.

(c) The probability of failure due to failing to emit, collect, or detect one or more photons during the remote gate operation, p_f.

These probabilities are determined by the physics of the sources and detectors.

Calculating the total cost of growing cluster states can be simplified by noting that, in the case of obtaining the insurance outcome, after applying the necessary single qubit corrections, one simply attempts the gate operation again. This process is repeated until a definite outcome (success or failure) is obtained. Thus, we can define *total* success and failure probabilities, P_s and P_f, of the corresponding definite outcomes after an (arbitrarily long) sequence of insurance outcomes. These probabilities are given by $P_s=\Sigma_{j=0}^{\infty}p_i^j p_s = p_s/(1-p_i)$ and $P_f=\Sigma_{j=0}^{\infty}p_i^j p_f=p_f/(1-p_i)$. The average number of attempted CZ operations required before we obtain a definite outcome is $N_{\mathrm{av}}=1/(1-p_i)$.

The overhead cost for making cluster states is then found using similar calculations to those presented in Refs. [44,79]. We first calculate the cost (i.e., the number of attempted CZ

operations per qubit in the final cluster) of generating linear clusters. If a CZ gate is repeatedly applied between the end qubits of two linear chains, each of length L_k, either the gate is (ultimately) successful, in which case the total length of the new cluster is $2L_k$, or the gate (ultimately) fails, in which case, the length of the original clusters shrinks by one qubit each. Repeatedly applying this procedure until a successful outcome is obtained (or until both original clusters are destroyed) [79] gives the expected length $L_{k+1}=\Sigma_{i=0}^{L_k}2(L_k-i)P_sP_f^i\approx 2L_k-2p_f/p_s$. Denoting the average number of attempts to create a chain of length L_k by N_k, we also have $N_{k+1}=2N_k+1/p_s$. Solving these recursion relations gives a total cost

$$N(L)=\frac{\left(N_0+\frac{1}{p_s}\right)\left(L-\frac{2p_f}{p_s}\right)}{\left(L_0-\frac{2p_f}{p_s}\right)}-\frac{1}{p_s}, \tag{39}$$

where N_0 denotes the cost of growing a short cluster of length L_0. Note that for the average cluster length to grow on each round of the protocol, we require $L_1>L_0$, which implies that the length of the short chains should satisfy $L_0>2p_f/p_s$.

Chains of fixed length L_0 can be grown independently using the probabilistic CZ operation, by joining subchains together. Growing these short chains adds a constant overhead cost to the cluster generation process. We use a divide and conquer approach to making these short chains [44,79], in which, on each round of the protocol, we attempt to join equal length pairs of linear clusters using the probabilistic CZ operation. If we obtain the insurance outcome on any such attempt, we try the operation again, whereas if we fail, we assume (for ease of calculation) that the short chains are discarded. On the kth round of this protocol, the length of the chains is $l_k=2^k$, and the number of attempted CZ operations is given by the recursion relation $n_k=2n_{k-1}/P_s+N_{\mathrm{av}}/P_s$. Solving these relations gives

$$N_0(L_0)=N_{\mathrm{av}}\sum_{i=1}^{\log_2 L_0}\frac{2^{i-1}}{P_s^i}. \tag{40}$$

Combining Eq. (39) and Eq. (40), one can calculate the total cost of growing linear clusters for given values of p_f, p_s, and p_i. For instance, taking $p_f=0.6$, $p_i=p_s=0.2$, we require $L_0>6$. Taking $L_0=2^3=8$, the total cost for making a linear cluster of length L is found to be $N(L)=185L-1115$ attempted CZ operations. A moderate increase in success probability can dramatically decrease the cost. Taking $p_f=0.4$, $p_i=p_s=0.3$, we require $L_0>2.67$, and taking $L_0=2^2=4$, we find the total cost to be $N(L)=16\frac{2}{3}L-47\frac{7}{9}$. Note that the negative constant term in these expressions is an artifact of joining small numbers of chains together to make an isolated chain of length L. This is an edge effect which should be neglected when considering the asymptotic cost of making long chains.

Linear clusters are not sufficient for simulating arbitrary logic networks [83], and therefore it is necessary to generate more general graph states. A variety of techniques for making such states using probabilistic entangling operations have been proposed, which include linking linear clusters using independently prepared "I" shaped clusters [44], using microclusters [15], using redundantly encoded qubits [16], or by making use of "+" shaped clusters [79]. Here, we propose a relatively efficient method for creating vertical bonds between linear cluster chains.

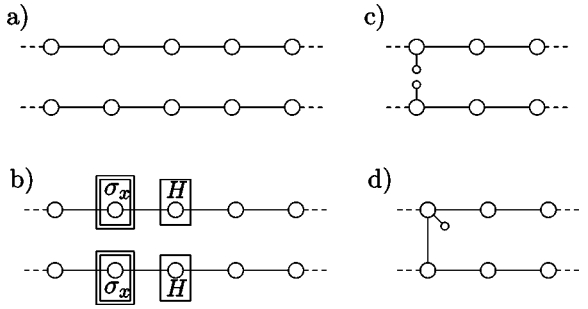

FIG. 7. Creating vertical bonds. (a) We start out with two sufficiently long cluster chains and we wish to create a vertical bond between the two qubits on the left. (b) We apply a σ_x measurement to the two adjacent qubits and a Hadamard operation H on the next. (c) This will result in a redundant encoding of the qubits we wish to bond together. (d) Applying the entangling operation to the dangling bonds or "cherries" will create the vertical bond. Note that we also removed the qubits in the vertical bond by applying another σ_x measurement resulting in another redundant encoding. If this procedure fails we are left with a shorter chain and we can try to create a vertical bond again.

We employ a technique based on that introduced by Browne and Rudolph [16], which involves four steps as shown in Fig. 7.

(a) First, we assume that we have sufficiently long linear cluster chains. These can be produced efficiently in the manner outlined above. In order to establish the amount of resources needed to create a vertical bond, we will count the number of qubits that are utilized on average in this process, as well as the average number of entangling operations.

(b) Second, we identify the two qubits that we wish to entangle with a vertical bond (in Fig. 7 the two left-most qubits). The qubits directly on the right of these qubits are then measured in the σ_x basis. A Hadamard operation on the third qubit in each chain returns the overal state to a graph state.

(c) This will result in dangling bonds or *cherries* [84] hanging from the two qubits that are to be connected. This is a form of redundant encoding, and it allows us to apply the entangling operation to the two cherries. In case of a failure, the entangling operation will *not* break the linear cluster chains. It will destroy only the cherries and as a result both chains are shortened by two qubits. Steps (b) and (c) can then be repeated.

(d) When the entangling operation succeeds, we have forged a vertical bond between the two qubits chosen in step (a). The vertical link is itself a chain of two qubits. These are typically not wanted, so we can remove one of them with a σ_x measurement creating another cherry in the other qubit in the chain. This redundancy can be pruned, but may also be useful for creating additional bonds, or may even be useful for error correction.

TABLE I. The average number of entangling operations per vertical bond, given by $N_{\text{bond}}=2N(M)+(1-p_i)/p_s$. Here p_s, p_f, and p_i are the success, failure, and insurance probabilities, respectively. $L_0=2^n$ is the length of the chain that is needed to obey the growth requirement, and N_0 is the number of EOs needed to achieve this length. M is the average cluster chain consumed by the forging of a vertical bond, and $N(M)$ is the number of EOs needed to achieve this length.

p_s	p_f	p_i	L_0	N_0	M	$N(M)$	N_{bond}
0.2	0.6	0.2	$2^3=8$	365	9	$185M$	3334
0.3	0.4	0.3	$2^2=4$	$18\frac{8}{9}$	$5\frac{2}{3}$	$16\frac{2}{3}M$	$191\frac{2}{9}$
0.4	0.2	0.4	$2^1=2$	$2\frac{1}{2}$	3	$5M$	$32\frac{1}{2}$
0.5	0.5	0	$2^2=4$	10	5	$6M$	62

We will now estimate the cost of this procedure. Since two qubits are burnt in each step, and we need to repeat the process P_s^{-1} times, the average length of each chain that is consumed in the bonding process is

$$M = 2P_s^{-1} + 1 = \frac{2(1-p_i)}{p_s} + 1, \tag{41}$$

where the extra +1 counts the qubits that will establish the vertical link. The number of entangling operations needed to make a vertical bond is then

$$N_{\text{bond}} = 2N(M) + P_s^{-1} = 2N(M) + \frac{(1-p_i)}{p_s}, \tag{42}$$

where the extra P_s^{-1} takes into account the number of entangling operations that are needed to link the cherries together into a vertical bond. In Table I we calculated the number of entangling operations that are needed to forge a vertical bond given several specific values for the success, failure, and insurance probabilities.

VI. CONCLUSIONS

We analyzed a hybrid architecture for quantum computing using stationary and flying qubits, which is based on our earlier work [43,44], in detail. It was shown that this approach solves some of the most pressing problems that arise in nonhybrid architectures. Our system is scalable, even with nonideal components, and more importantly, it uses no direct qubit-qubit interactions. This means that the qubits will be subject to less decoherence and fewer control errors. When realistic photodetectors are used, photon loss will affect only the efficiency of the scheme. Furthermore, our system relies on components that have been demonstrated in experiment, and is largely implementation independent. Despite the no-go theorem for optical Bell-state measurements, it is in principle possible to implement a deterministic gate between distant qubits.

However, when losses are taken into account, the gate becomes necessarily probabilistic. In order to achieve robustness against general decoherence and to guarantee high fidelities, we showed how to construct cluster or graph states using the two-qubit gate. Our entangling operation, which produces the bonds in the graph states, is not limited to physically adjacent matter qubits. As a consequence, no extensive swapping operations need to be taken into account in the production of nontrivial graph states. This architecture for quantum computation is inherently distributed, and hence can be used for integrated quantum computation and communication purposes.

ACKNOWLEDGMENTS

Y.L.L., A.B., and L.C.K. thank H. J. Briegel, A. Browaeys, D. E. Browne, T. Durt, A. K. Ekert, P. Grangier, M. Jones, and P. L. Knight for stimulating discussions. P.K. and S.D.B. thank S. Benjamin, J. Eisert, B. Lovett, M. A. Nielsen, and T. Stace for fruitful discussions and particularly D. Browne for giving them a deeper insight into cluster state generation. Y.L.L. acknowledges funding from the DSO National Laboratories in Singapore and A.B. acknowledges support from the Royal Society and the GCHQ. This work was supported in part by the European Union (RAMBOQ, QGATES) and the UK Engineering and Physical Sciences Research Council (QIP IRC).

[1] P. W. Shor, *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, California, 1994), p. 124.

[2] D. Deutsch, Proc. R. Soc. London, Ser. A **400**, 97 (1985).

[3] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, Nature (London) **414**, 883 (2001).

[4] F. Jelezko, T. Gaebel, I. Popa, M. Domhan, A. Gruber, and J. Wrachtrup, Phys. Rev. Lett. **93**, 130501 (2004).

[5] F. Schmidt-Kaler, H. Häffner, M. Riebe, S. Gulde, G. P. T. Lancaster, T. Deuschle, C. Becher, C. F. Roos, J. Eschner, and R. Blatt, Nature (London) **422**, 408 (2003).

[6] D. Leibfried, B. DeMarco, V. Meyer, D. Lucas, M. D. Barrett, J. Britton, W. M. Itano, B. Jelenkovic, C. Langer, T. Rosenband, and D. J. Wineland, Nature (London) **422**, 412 (2003).

[7] M. Riebe, H. Häffner, C. F. Roos, W. Hansel, J. Benhelm, G. P. T. Lancaster, T. W. Korber, C. Becher, F. Schmidt-Kaler, D. F. V. James, and R. Blatt, Nature (London) **429**, 734 (2004).
[8] J. Chiaverini, D. Leibfried, T. Schaetz, M. D. Barrett, R. B. Blakestad, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, R. Ozeri, and D. J. Wineland, Nature (London) **432**, 602 (2004).
[9] D. Kielpinski, C. Monroe, and D. J. Wineland, Nature (London) **417**, 709 (2002).
[10] C. H. Bennett and G. Brassard, *Proceeding of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, 1984 (IEEE, New York, 1984), p. 175; IBM Tech. Discl. Bull. **28**, 3153 (1985).
[11] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[12] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
[13] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[14] N. Yoran and B. Reznik, Phys. Rev. Lett. **91**, 037903 (2003).
[15] M. A. Nielsen, Phys. Rev. Lett. **93**, 040503 (2004).
[16] D. E. Browne and T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005).
[17] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, Nature (London) **434**, 169 (2005).
[18] R. M. Gingrich, P. Kok, H. Lee, F. Vatan, and J. P. Dowling, Phys. Rev. Lett. **91**, 217901 (2003).
[19] L. K. Grover, Bell Labs Technical Memorandum No. ITD-96-30115J, e-print quant-ph/9607024.
[20] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, Phys. Rev. A **59**, 4249 (1999).
[21] J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio, Phys. Rev. A **62**, 052317 (2000).
[22] L.-M. Duan, B. B. Blinov, D. L. Moehring, and C. Monroe, Quantum Inf. Comput. **4**, 165 (2004).
[23] J. M. Taylor, G. Giedke, H. Christ, B. Paredes, J. I. Cirac, P. Zoller, M. D. Lukin, and A. Imamoglu, e-print cond-mat/0407640.
[24] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, Phys. Rev. Lett. **78**, 3221 (1997).
[25] S. J. van Enk, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **78**, 4293 (1997).
[26] A. Sørensen and K. Mølmer, Phys. Rev. A **58**, 2745 (1998).
[27] M. N. Leuenberger, M. E. Flatte, and D. D. Awschalom, Phys. Rev. Lett. **94**, 107401 (2005).
[28] Y.-F. Xiao, X.-M. Lin, J. Gao, Y. Yang, Z.-F. Han, and G.-C. Guo, Phys. Rev. A **70**, 042314 (2004).
[29] X.-F. Zhou, Y.-S. Zhang, and G.-C. Guo, Phys. Rev. A **71**, 064302 (2005).
[30] S. Mancini and S. Bose, Phys. Rev. A **70**, 022307 (2004).
[31] J. D. Franson, B. C. Jacobs, and T. B. Pittman, Phys. Rev. A **70**, 062302 (2004).
[32] S. D. Barrett, P. Kok, K. Nemoto, R. G. Beausoleil, W. J. Munro, and T. P. Spiller, Phys. Rev. A **71**, 060302(R) (2005).
[33] C. Cabrillo, J. I. Cirac, P. Garcia-Fernandez, and P. Zoller, Phys. Rev. A **59**, 1025 (1999).
[34] S. Bose, P. L. Knight, M. B. Plenio, and V. Vedral, Phys. Rev. Lett. **83**, 5158 (1999).
[35] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).
[36] L.-M. Duan and H. J. Kimble, Phys. Rev. Lett. **90**, 253601 (2003).
[37] D. E. Browne, M. B. Plenio, and S. F. Huelga, Phys. Rev. Lett. **91**, 067901 (2003).
[38] C. Simon and W. T. M. Irvine, Phys. Rev. Lett. **91**, 110405 (2003).
[39] Y. L. Lim and A. Beige, J. Phys. A **38**, L7 (2005).
[40] X. B. Zou and W. Mathis, Phys. Rev. A **71**, 042334 (2005).
[41] G. Chimczak, R. Tanas, and A. Miranowicz, Phys. Rev. A **71**, 032316 (2005).
[42] I. E. Protsenko, G. Reymond, N. Schlosser, and P. Grangier, Phys. Rev. A **66**, 062306 (2002); N. Schlosser, I. E. Protsenko and P. Grangier, Philos. Trans. R. Soc. London, Ser. A **361**, 1527 (2003).
[43] Y. L. Lim, A. Beige, and L. C. Kwek, Phys. Rev. Lett. **95**, 030505 (2005).
[44] S. D. Barrett and P. Kok, Phys. Rev. A **71**, 060310(R) (2005).
[45] B. B. Blinov, D. L. Moehring, L.-M. Duan, and C. Monroe, Nature (London) **428**, 153 (2004).
[46] M. Weber, Ph.D. thesis, Ludwig-Maximilian-Universität München 2005.
[47] M. Hennrich, T. Legero, A. Kuhn, and G. Rempe, Phys. Rev. Lett. **85**, 4872 (2000); A. Kuhn, M. Hennrich, and G. Rempe, *ibid.* **89**, 067901 (2002).
[48] O. Benson, C. Santori, M. Pelton, and Y. Yamamoto, Phys. Rev. Lett. **84**, 2513 (2000); M. Pelton, C. Santori, J. Vuckovic, B. Zhang, G. S. Solomon, J. Plant, and Y. Yamamoto, *ibid.* **89**, 233602 (2002).
[49] J. McKeever, A. Boca, A. D. Boozer, R. Miller, J. R. Buck, A. Kuzmich, and H. J. Kimble, Science **303**, 1992 (2004).
[50] M. Keller, B. Lange, K. Hayasaka, W. Lange, and H. Walther, Nature (London) **431**, 1075 (2004).
[51] D. N. Matsukevich and A. Kuzmich, Science **306**, 663 (2004).
[52] B. Darquie, M. P. A. Jones, J. Dingjan, J. Beugnon, S. Bargamini, Y. Sortais, G. Messin, A. Browaeys, and P. Grangier, Science **309**, 454 (2005).
[53] D. Rosenberg, A. E. Lita, A. J. Miller, and S. W. Nam, Phys. Rev. A **71**, 061803(R) (2005).
[54] D. Gottesman, J. Mod. Opt. **47**, 333 (2000).
[55] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).
[56] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).
[57] M. A. Nielsen, Phys. Lett. A **308**, 96 (2003).
[58] A. M. Childs, D. W. Leung, and M. A. Nielsen, Phys. Rev. A **71**, 032318 (2005).
[59] A. Beige, D. Braun, B. Tregenna, and P. L. Knight, Phys. Rev. Lett. **85**, 1762 (2000).
[60] A. Beige, Phys. Rev. A **69**, 012303 (2004).
[61] G. G. Lapaire, P. Kok, J. P. Dowling, and J. E. Sipe, Phys. Rev. A **68**, 042314 (2003).
[62] D. DiVincenzo, in *Scalable quantum computers; paving the way to realization*, edited by S. L. Braunstein and H.-K. Lo (Wiley-VCH, Berlin, 2001).
[63] This gate can be easily accomplished by applying a strongly detuned laser field for a certain time t.
[64] L. Vaidman and N. Yoran, Phys. Rev. A **59**, 116 (1999); N. Lütkenhaus, J. Calsamiglia, and K. A. Suominen, *ibid.* **59**, 3295 (1999).
[65] K. M. Gheri, C. Saavedra, P. Törmä, J. I. Cirac, and P. Zoller,

Phys. Rev. A **58**, R2627 (1998).
[66] C. K. Law, and H. J. Kimble, J. Mod. Opt. **44**, 2027 (1997); A. Kuhn, M. Hennrich, T. Bondo, and G. Rempe, *ibid.* **69**, 373 (1999).
[67] M. Zukowski, A. Zeilinger, and M. A. Horne, Phys. Rev. A **55**, 2564 (1997).
[68] P. Kok and S. L. Braunstein, Phys. Rev. A **63**, 033812 (2001).
[69] A. M. Steane, Phys. Rev. A **68**, 042322 (2003).
[70] E. Knill, Nature (London) **434**, 39 (2005).
[71] M. Varnava, D. E. Browne, and T. Rudolph, e-print quant-ph/0507036.
[72] T. C. Ralph, A. J. F. Hayes, and A. Gilchrist, Phys. Rev. Lett. **95**, 100501 (2005).
[73] S. Takeuchi, J. Kim, Y. Yamamoto, and H. H. Hoguer, Appl. Phys. Lett. **74**, 1063 (1999).
[74] T. Legero, T. Wilk, M. Hennrich, G. Rempe, and A. Kuhn, Phys. Rev. Lett. **93**, 070503 (2004).
[75] Perkin-Elmer data sheet, available at http://optoelectronics.perkinelmer.com/content/Datasheets/SPCM-AQR.pdf
[76] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[77] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004).
[78] Y. S. Weinstein, C. S. Hellberg, and J. Levy, Phys. Rev. A **72**, 020304(R) (2005).
[79] L.-M. Duan and R. Raussendorf, Phys. Rev. Lett. **95**, 080503 (2005).
[80] S. C. Benjamin, Phys. Rev. A **72**, 056302 (2005).
[81] S. C. Benjamin, J. Eisert, and T. Stace, New J. Phys. **7**, 194 (2005).
[82] Q. Chen, J. Cheng, K.-L. Wang, and J. Du, e-print quant-ph/0507066.
[83] M. A. Nielsen, e-print quant-ph/0504097, Rev. Math. Phys. (to be published).
[84] Terminology introduced by T. M. Stace.