Deterministic Linear Optics Quantum Computation with Single Photon Qubits

N. Yoran and B. Reznik

School of Physics and Astronomy, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel-Aviv University, Tel-Aviv 69978, Israel

(Received 27 February 2003; published 17 July 2003)

We suggest an efficient scheme for quantum computation with linear optical elements, where the qubits are encoded in single photon states. The scheme reduces the resources required per logical gate by several orders of magnitude, compared to an earlier proposal of Knill, Laflamme, and Milburn, while the resource overhead per gate is independent of the length of the computation. A central feature of the scheme, enabling these improvements, is the prior construction of a "linked" photon state designed according to the particular quantum circuit one wishes to process. Once this state has been successfully prepared, the computation is pursued deterministically by a sequence of teleportation steps.

DOI: 10.1103/PhysRevLett.91.037903 PACS numbers: 03.67.Pp, 03.67.Lx, 42.50.Dv

Optical systems have proven to be a very successful tool for implementing quantum information and communication tasks such as quantum cryptography, teleportation, and quantum dense coding [1]. However, when it comes to more complicated protocols, let alone scalable quantum computation, such systems suffer from a major disadvantage—the lack of interaction between photons that is needed for implementation of conditional two-qubits logic gates. In a recent work, Knill, Laflamme, and Milburn (KLM) [2] proposed a scheme for quantum computation based on linear optics, demonstrating that this obstacle can be overcome. A two-qubit gate is performed, according to this scheme, in two stages. First, a standard ancillary state is prepared and subjected to some gates. This off-line preparation step may succeed with low probability (as it relies on postselection). In the second stage, the prepared state can be used to apply a logical gate on the input state by means of the teleportation scheme suggested by Gottesman and Chuang [3]. This second step is again probabilistic but with a success rate that can be made arbitrarily close to unity, depending on the resources (in terms of the number of elementary operations) used in the preparation. In addition to the above elements, the KLM scheme necessitates the use of quantum error correcting codes to avoid an exponential increase in resources for success probability approaching one. Nevertheless, the scheme is yet inefficient as it requires an enormous resource overhead to overcome the unavoidable finite error occurring in each gate application.

In this Letter, we suggest a new scheme for quantum computation with ideal (error free) linear optical elements. A key point in our scheme is the introduction of a multiphoton entangled linked photon state whose structure is dictated by the form of the quantum circuit that one wishes to construct. This state is prepared by employing KLM-type postselected gates. However, once the state has been successfully constructed, the remaining computation process, which utilizes a deterministic teleportation scheme, can be ideally completed with unit probability. This would allow us to encode the qubits in a single degree of freedom (polarization) of single photons. Moreover, the required number of elementary operations per logical gate will be dramatically reduced. In the proposed scheme, five successful applications of a KLM-type gate are sufficient for implementing a logical two-qubit gate while, in the KLM approach, 200 successful applications of the same gate implement the logical gate with about 5% intrinsic error probability.

The teleportation protocol employed here uses an extension of the idea proposed by Popescu [4] and experimentally realized by Boschi *et al.* [5]. In this method, a pair of EPR entangled photons is utilized, and both the teleported state and "half" of the EPR state are associated with a single photon. Consequently, linear optics elements are sufficient for implementing a complete Bell-state measurement. We begin by extending this scheme to a chain of photons where each photon is entangled with two nearest neighbor photons. Let us denote by $p_1, p_2, \ldots, p_{n+1}$ the photons, and consider the following *chain state*:

$$\chi_{p_1}(|1\rangle_{p_1}|\updownarrow\rangle_{p_2} + |2\rangle_{p_1}|\leftrightarrow\rangle_{p_2})(|3\rangle_{p_2}|\updownarrow\rangle_{p_3} + |4\rangle_{p_2}|\leftrightarrow\rangle_{p_3})\cdots(|2n-1\rangle_{p_n}|\updownarrow\rangle_{p_{n+1}} + |2n\rangle_{p_n}|\leftrightarrow\rangle_{p_{n+1}})|2n+1\rangle_{p_{n+1}}. \quad (1)$$

$\chi_{p_1} = (\alpha|\updownarrow\rangle_{p_1} + \beta|\leftrightarrow\rangle_{p_1})$ is an arbitrary polarization state of the first photon in the chain, and $|m\rangle$ and $|\updownarrow, \leftrightarrow\rangle$ denote the position and polarization states of the photons, respectively. The chain state, depicted schematically in Fig. 1, manifests pairwise maximal entanglement, which we shall refer to as a *link*, between the path of p_i and the polarization of the next photon p_{i+1}, and so forth.

The above state can be used to teleport the state $|\chi\rangle_{p_1}$ through the whole chain by means of N separate

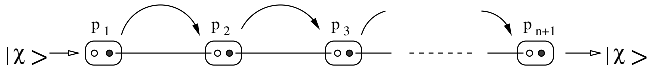

FIG. 1. Schematic description of a single chain state with $n + 1$ photons. A rectangle indicates a photon, whose polarization and path degree of freedom are denoted by empty and full circles, respectively. The linking horizontal lines denote the entanglement between position and polarization. The arrows portray the teleportation sequence of the state χ to the last photon in the chain.

teleportation steps. In each step, polarizing beam splitters (BPS) are utilized for a path-polarization Bell measurement on photon p_i. This sends the state χ (after correcting p_{i+1}) to the polarization state of the next photon (p_{i+1}). By N such sequential teleportation steps, $|\chi\rangle$ is teleported to the last photon in the chain.

We shall use one such chain to represent the "world line" of a single qubit in a quantum circuit. The time step corresponds here to teleportation steps. Hence, for a circuit with N input qubits, we will use N chains. To include the required gates, we next introduce gates between photons of different chains. Since the teleportation of the input state sends χ to polarization states, we need to apply the gate between the polarization states of the appropriate photons in each chain. However, as was shown by Gottesman and Chuang [3], one can reverse the order of teleportation and gate operations. When we first apply the gate operation, in order to receive the same output (as in the original order), different corrections must be applied; however, these would still be one-qubit corrections which can be implemented with linear optics. Thus, we will first apply the relevant gates on the different chains, producing a new state (henceforth referred to as a linked state) in which each photon in a chain is entangled to another photon of a different chain, and later teleport the input state through the linked state.

To exemplify this construction, consider the three qubit circuit depicted in Fig. 2, which sends $\chi_{1,2,3} \rightarrow G_{1,2}G_{1,3}G_{1,2}\chi_{1,2,3}$. We replace this circuit with the linked state depicted in Fig. 3, which can be constructed as follows. We begin with three chain states, $|\mathrm{I}\rangle = |p_1, p_2, p_3, p_4\rangle_I$, $|\mathrm{II}\rangle = |p_1, p_2, p_3\rangle_{II}$, and $|\mathrm{III}\rangle = |p_1, p_2\rangle_{\mathrm{III}}$. The gates are then applied on the polarization states according to $|\mathrm{I}, \mathrm{II}, \mathrm{III}\rangle \rightarrow G(\mathrm{I}_{p_4}, \mathrm{II}_{p_3})G(\mathrm{I}_{p_3}, \mathrm{III}_{p_2})G(\mathrm{I}_{p_2}, \mathrm{II}_{p_2})|\mathrm{I}, \mathrm{II}, \mathrm{III}\rangle$, where I_{p_2} denotes the polarization states of the second photon in the first chain, etc. Next, in order to perform the computation, we introduce the input state χ by rotating the polarization of the first photon in each chain (assuming for the time being that χ is a nonentangled, known state). Then we teleport χ through the linked state and apply the relevant single qubit corrections.

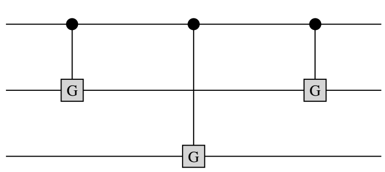

FIG. 2. A simple circuit with three qubits and gate operations.

Our scheme generalizes to any quantum circuit, where the number of links in each chain is determined by the number of gates that are applied on that particular qubit. We next address the preparation process in detail.

Preparation of linked states.—The off-line part of the computation consists of two basic operations: addition of a new link to each chain, and application of a two-qubit gate between polarization states of different chains. We next show how these two operations may be performed by applying the KLM postselected nondeterministic conditional phase flip gates. In principle, we can use any of the gates designed by KLM (as well as the improvements suggested in [6,7]). We will refer to these implementations of the conditional phase flip as a CZ gate. These gates operate on the path degree of freedom of photons all with identical polarization. This poses no difficulty in our case, because we can easily move the information carried by polarization states back and forth between the path and polarization degrees of freedom by employing polarizing beam splitters and polarization rotation plates.

Consider the construction of a new link to one of the chains (Fig. 4). To achieve that, we apply a gate between the path degree of freedom of the last photon in the chain and the polarization of an additional photon. Suppose that b is the last photon in the chain $(|1\rangle_a|\updownarrow\rangle_b + |2\rangle_a|\leftrightarrow\rangle_b)|3\rangle_b$. We now add photon c in a state $(|5\rangle_c + |6\rangle_c)|\updownarrow\rangle_c$. Transmitting mode $|3\rangle_b$ through a 50/50 beam splitter (splitting it to 3 and 4) and applying polarizing beam splitters (PBS), we obtain

$$|1\rangle_a|\updownarrow\rangle_b(|3\rangle_b + |4\rangle_b) + |2\rangle_a|\leftrightarrow\rangle_b(|3'\rangle_b + |4'\rangle_b). \quad (2)$$

Notice that 3,4 and $3', 4'$ carry different polarizations; hence, we next apply CZ in two consecutive steps. First between the pair $\{3, 4\}_b$ and $\{5, 6\}_c$, followed by a 50/50 beam splitter to 3 and 4. This takes the state of the four modes to $|3\rangle_b|5\rangle_c + |4\rangle_b|6\rangle_c$. In the second step, the polarization of modes $3'$ and $4'$ is rotated (so it matches the polarization of c) and the procedure is repeated for $\{3', 4'\}_b$. A successful sequence of (two) gate operations

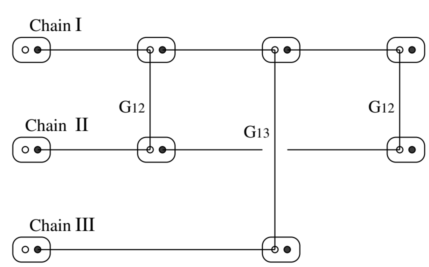

FIG. 3. A schematic description of the linked state that is needed for generating the quantum circuit in Fig. 2. The vertical lines represent the entanglement that is produced by applying the gates—$G_{i,j}$.

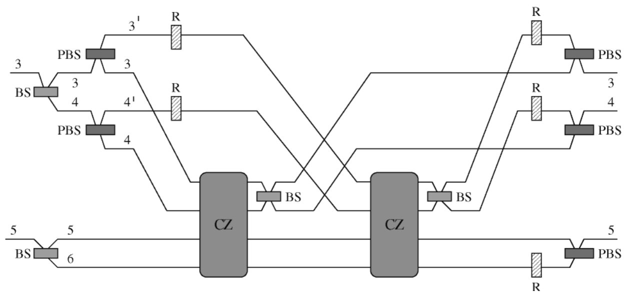

FIG. 4. Addition of a link to a chain by the use of two CZ gates. The additional elements are 50/50 beam splitters (BS), polarizing beam splitters (PBS), and rotating wave plates (R).

creates a link between b and c. Finally, the entanglement is transferred to the required path-polarization form:

$$\cdots \times (|1\rangle_a|\updownarrow\rangle_b + |2\rangle_a|\leftrightarrow\rangle_b)(|3\rangle_b|\updownarrow\rangle_c + |4\rangle_b|\leftrightarrow\rangle_c)|5\rangle_c. \tag{3}$$

Having constructed the relevant links, we next consider a two-qubit gate (Fig. 5). In principle, the gate can be applied after completing the construction of the chains. However, as we apply the gate to the polarization of photons which are entangled to other photons in the chain, this would require the application of four CZ gates for each logic gate. It would therefore be more efficient to apply the gates to the proper photons immediately after these links have been established, before the next links in each chain are produced. As the last photon in each chain

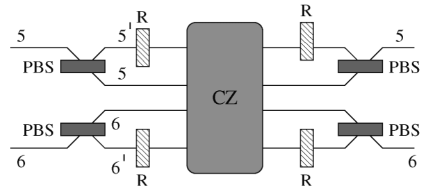

FIG. 5. Conditional phase flip on two photons of two different chains with a single CZ operation.

is located in a single mode, the operation can be implemented by a single CZ application. Suppose that we want to apply a two-qubit gate between the polarization states of photons b and d in the chain states

$$\begin{aligned} &\cdots \times (|1\rangle_a|\updownarrow\rangle_b + |2\rangle_a|\leftrightarrow\rangle_b)|5\rangle_b \quad \text{and} \\ &\cdots \times (|3\rangle_c|\updownarrow\rangle_d + |4\rangle_c|\leftrightarrow\rangle_d)|6\rangle_d. \end{aligned} \tag{4}$$

Employing a PBS for each chain and rotating the polarization of the modes corresponding to the horizontal modes ($5'$ and $6'$), we obtain

$$\begin{aligned} &\cdots \times |\updownarrow\rangle_b(|1\rangle_a|5\rangle_b + |2\rangle_a|5'\rangle_b) \quad \text{and} \\ &\cdots \times |\updownarrow\rangle_d(|3\rangle_c|6\rangle_d + |4\rangle_c|6'\rangle_b). \end{aligned} \tag{5}$$

At this point, we can apply the CZ gate which produces a conditional phase flip (other two-qubit gates are equivalent up to singe-qubit operations). Finally, we transfer the entanglement between photons in each pair $\{a, b\}$ and $\{c, d\}$ back to the path-polarization form. A successful CZ gate operation would leave us in the desired state:

$$(|1\rangle_a|\updownarrow\rangle_b|3\rangle_c|\updownarrow\rangle_d + |1\rangle_a|\updownarrow\rangle_b|4_c\rangle|\leftrightarrow\rangle_d + |2\rangle_a|\leftrightarrow\rangle_b|3\rangle_c|\updownarrow\rangle_d - |2\rangle_a|\leftrightarrow\rangle_b|4\rangle_c|\leftrightarrow\rangle_d)|5\rangle_b|6\rangle_d. \tag{6}$$

Efficient construction of large circuits.—A basic building block of the KLM scheme is a conditional phase flip gate that employs interference of input photons and ancillary photons and postselection. This basic gate operates successfully with probability 1/16. In our scheme, this gate can be used for generating small circuits. However, for long enough quantum circuits the preparation process becomes inefficient, and gates with higher success rate must be employed. In the construction of the overall linked state, we proceed step by step, since a failure in the gate operation in one step might destroy previously constructed links and gates; in order to progress the combined process of link/gate generation must succeed with probability larger than 1/2. This can be achieved by replacing the basic CZ gates with an improved gate version proposed by KLM (for a recent improvement, see [8]). These gates operate through the application of a new type of teleportation protocol based on the $n+1$ point Fourier transform ($\hat{F}_{n+1}$), which operates successfully with probability $n/(n+1)$. This gate, $CZ_{n^2/(n+1)^2}$, is constructed of two independent $\hat{F}_{n+1}$-based teleportations and therefore operates successfully with probability $n^2/(n+1)^2$. The application of each $CZ_{n^2/(n+1)^2}$ requires that a special ancillary state of $2n$ photons in $4n$ modes would be prepared in advance (by utilizing basic CZ gates). Thus, the preparation stage of our scheme has two parts. In the first part, we prepare independent small-scale ancillary states with which we apply, in the second part, the $CZ_{n^2/(n+1)^2}$ gates to construct the overall linked state.

The $CZ_{n^2/(n+1)^2}$ fails when either one of the independent teleportation protocols fails. A failure of the teleportation protocol results in the measurement of the teleported qubit. Let us consider the operation of applying a gate between two chains. By inspecting Eq. (5), it is clear that failure in teleporting photon b would leave photon a in either mode 1 or mode 2 breaking the link. In the same way, failure in teleporting photon d would brake its corresponding link. Clearly, it would be more efficient to apply the two teleportation protocols in a sequence, where the second is applied only if the first has succeeded, eliminating the possibility of breaking two links. Thus, in applying a gate, the probability of success is $p = n^2/(n+1)^2$ while with probability $(1-p)$ one link is broken.

In adding a link to a chain, we apply two CZ operations. These are applied to one photon (in four modes) which constitutes the last link of a chain, together with a newly introduced photon. As this new photon is not entangled to any chain, there is no point in wasting an $\hat{F}_{n+1}$-based teleportation protocol on it. This photon can be prepared as part of the ancilla. Therefore, each of the CZ operations in adding a link will be carried out through the application of a half $CZ_{n^2/(n+1)^2}$ gate in which a pair of modes [3 and 4 in (2) and afterwards $3'$ and $4'$] undergoes teleportation, but the other pair (5 and 6) does not. The CZ is applied to this pair of modes together with the components of the ancilla in the first part of the preparation. The ancillary state [2] for one $\hat{F}_{n+1}$-based teleportation is $|t_n\rangle = \sum_{j=0}^{n} |1\rangle^j |0\rangle^{n-j} |0\rangle^j |1\rangle^{n-j}$, defining a modified $|t_n\rangle$ as $|\tilde{t}_n\rangle = \sum_{j=0}^{n} (-1)^j |1\rangle^j |0\rangle^{n-j} |0\rangle^j |1\rangle^{n-j}$ The ancillary state for the two CZ operations would be

$$|5\rangle|\tilde{t}_n\rangle_1|\tilde{t}_n\rangle_2 + |6\rangle|t_n\rangle_1|t_n\rangle_2, \qquad (7)$$

where 1 and 2 denote the states used for the teleportation of modes $\{3, 4\}$ and $\{3', 4'\}$ respectively. In this case, the overall process can fail in two ways. If a maximal number of photons is detected at the outputs of the $\hat{F}_{n+1}$ operation (thus destroying also the teleported photon), then the previous link is destroyed together with the gate operation that was applied to it. If no photon is detected, the entanglement is not completely destroyed and we can still bring the system back to the initial state. Thus, the whole process (the two teleportation protocols) succeeds with probability $p = n^2/(n+1)^2$ and in the case of failure we have the same probability $((1-p)/2)$ to either destroy the previous link (together with the gate operation) or to remain in the same initial state.

Employing our scheme for every logic gate in the required computation, we need to perform six successful $\hat{F}_{n+1}$-based teleportation protocols, which are equivalent to three $CZ_{n^2/(n+1)^2}$ gates (two for adding two links to two different chains and one for applying the gate to those links). $n = 3$ is the smallest value for which the step-by-step construction of the linked state can advance forward with higher probability than moving backwards. In a computer simulation of a construction process for a two-qubit linked state (a two-qubit circuit), we obtained the average number of gates per logical gate, of ~ 220 for a $CZ_{9/16}$ gate, and ~ 15 for a $CZ_{16/25}$ gate. The large average number required for the case of the $CZ_{9/16}$ results from an overall probability very close to $1/2$ to advance forward. This number can be significantly reduced if we change the overall construction by adding inert links to the chains, i.e., photons on which no gate operation is applied. In this case, for a qubit that takes part in n two-qubit gates, we construct a chain of $2n$ links while the gates are applied to every second link. The only purpose of the inert links is to prevent a possible failure from spreading backwards, destroying previously constructed links and gates (if the step of adding a second link fails destructively then only the previous link is destroyed—the previous gate is not affected). Using this type of construction, we need five successful gate operations for every logic gate. Applying a computer simulation on a pair of chains, we obtain $\sim 23 CZ_{9/16}$ applications on average for every logic gate. The gate $CZ_{4/9}$ can be used as well by introducing additional inert links (at least three) for each gate.

It should be noted that for large scale linked states we can start the computation before the completion of the preparation. The computation is then carried out simultaneously with the construction of the linked state, where a "safety margin" (whose length, in terms of the number of links, would probably depend on the length of the computation) is maintained, keeping the probability for a sequence of failures that could destroy part of the data negligible. This method is more economical in terms of the required quantum storage capacity, as only a part of the complete linked state is kept at a given instance [9].

Thus far, we have assumed that the input is received classically. Given an arbitrary photon as an input we can teleport its state to the head of the chain by a Bell measurement. This measurement can be accomplished by applying a CZ gate together with additional one-qubit operations. Clearly, as this operation involves the actual input, the applied CZ gate must be one with a very high success rate. However, this operation is carried out only once for each qubit.

In the present scheme each photon carries two qubits. To achieve that we utilized both polarization and path degree of freedom. This led to a simple path-polarization factorization of the linked state (1). However, our scheme does not require the use of polarization. It has been shown that a linear optical realization exists for any $N \times N$ unitary matrix [10]. We can therefore represent the chain state (1) in terms of path degrees of freedom alone, by attributing four possible modes to each photon.

We thank Lev Vaidman for very helpful discussions, and acknowledge support from the Israel Science Foundation (Grant No. 62/01-1), and MOD Research and Technology Unit.

[1] D. Bouwmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information* (Springer-Verlag, Berlin, 2000).
[2] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
[3] D. Gottesman and I. Chuang, Nature (London) **402**, 309 (1999).
[4] S. Popescu, quant-ph/9501020.
[5] D. Boschi *et al.*, Phys. Rev. Lett. **80**, 1121 (1998).
[6] T. C. Ralph, A. G. Munro, and G. J. Milburn, Phys. Rev. A **65**, 012314 (2002).
[7] E. Knill, Phys. Rev. A **66**, 052306 (2002).
[8] J. D. Franson *et al.*, Phys. Rev. Lett. **89**, 137901 (2002).
[9] We thank E. Knill for bringing this to our attention.
[10] M. Reck *et al.*, Phys. Rev. Lett. **73**, 58 (1994).