Towards Scalable Linear-Optical Quantum Computers

J. P. Dowling,[1,5] **J. D. Franson,**[2] **H. Lee,**[1,4] **and G. J. Milburn**[3]

Scalable quantum computation with linear optics was considered to be impossible due to the lack of efficient two-qubit logic gates, despite the ease of implementation of one-qubit gates. Two-qubit gates necessarily need a non-linear interaction between the two photons, and the efficiency of this non-linear interaction is typically very small in bulk materials. However, it has recently been shown that this barrier can be circumvented with effective non-linearities produced by projective measurements, and with this work linear-optical quantum computing becomes a new avenue towards scalable quantum computation. We review several issues concerning the principles and requirements of this scheme.

1. PRINCIPLES

There are three key principles in the Knill, Laflamme, and Milburn (KLM) proposal[1] for efficient and scalable linear-optical quantum information processing (QIP):

(1) Conditional non-linear gates for two photon states.
(2) Teleportation to achieve high efficiency.
(3) Error correction to achieve scalability.

---

[1]Quantum Computing Technologies Group, Section 367, Jet Propulsion Laboratory, MS 126-347 and California Institute of Technology, 4800 Oak Grove Drive, CA 91109, USA.
[2]Applied Physics Laboratory, Johns Hopkins University, Laurel, MD 20723, USA.
[3]Centre for Quantum Computer Technology, University of Queensland, QLD 4072, Australia.
[4]To whom correspondence should be addressed.
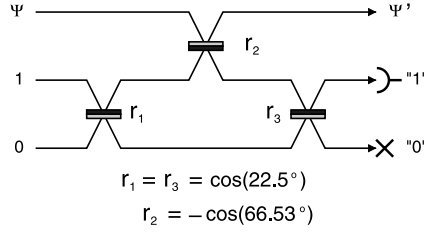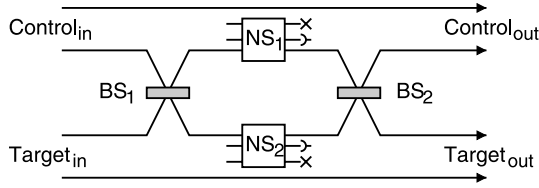[5]Department of Physics, Louisiana State University, Baton Rouge, LA 70803, USA.

Fig. 1.   The conditional non-linear sign (NS) gate.

Fig. 2.   Controlled-σ_z gate with dual-rail logic and two NS gates.

Conditional non-linear gates are based on the non-unitary state change due to measurement. The gate works with some probability, but correct functioning is heralded by the measurement result. We seek to implement a non-linear transformation, the so-called non-linear sign (NS) gate, on an arbitrary two-photon state of a single mode field:

$$|\psi\rangle = \alpha_0|0\rangle_1 + \alpha_1|1\rangle_1 + \alpha_2|2\rangle_1 \rightarrow |\psi'\rangle = \alpha_0|0\rangle_1 + \alpha_1|1\rangle_1 - \alpha_2|2\rangle_1. \qquad (1)$$

This is done using the linear-optical network shown in Fig. 1. The signal state is first combined with two ancilla modes, one in a single-photon state and one in the vacuum. At the end of the optical processing photon counting is done on the ancilla modes. If the number of photons is unchanged from the input, the desired transformed state exits the signal mode port. This will happen with a probability of 0.25.

In order to use this result to implement QIP we code the logical states as physical qubits using one photon in one of two modes: $|0\rangle_L = |1\rangle_1 \otimes |0\rangle_2, |1\rangle_L = |0\rangle_1 \otimes |1\rangle_2$. Single-qubit gates are then implemented by a beam splitter. A two qubit gate, the conditional sign-flip gate, can then be implemented using the Hong-Ou-Mandel (HOM) interference effect to first convert two single modes, each with one photon, into an appropriate entangled two-photon state (Fig. 2). Such a gate uses two NS gates and thus succeeds with probability of 0.125. A general formalism for calculating the effective photon non-linearities generated by such conditional measurement schemes in linear optics can be found in Ref. 2

We have also shown that probabilistic quantum logic operations can be performed using polarization-encoded qubits,[3] as illustrated by the controlled-NOT gate shown in Fig. 3. This device consists of two polarizing beam splitters and two polarization-sensitive detectors, along with a pair of entangled ancilla photons.

The correct controlled-NOT logic operation will have been performed whenever one and only one photon is detected in each of the two detectors, which occurs with a probability of 0.25. Feed-forward control[4] must also be applied, depending on what polarization states were measured. From an experimental perspective, this approach has the advantage of being relatively simple and insensitive to phase drifts.

A sequence of such probabilistic gates is of course not scalable. However, the Gottesman and Chuang protocol for implementing gates via teleportation[5] can be used to fix this. Implementation of the gate then reduces to preparing the appropriate entangled-state resource. That can be done off-line by using conditional gates, and only when success is achieved is the teleportation gate completed. Using a resource with n photons in $2n$ modes decreases the gate failure probability as n^{-1} or even as n^{-2}.[6] Gates can thus be implemented efficiently. The controlled-σ_z (CZ) gate is now achieved with success probability $n^2/(n+1)^2$, denoted as $CZ_{n^2/(n+1)^2}$.
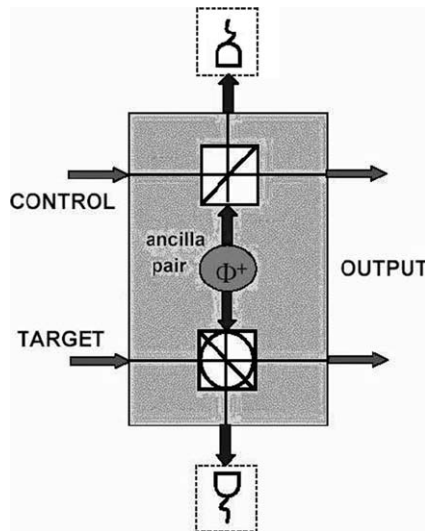

Fig. 3. Implementation of a probabilistic controlled-NOT gate using polarization-encoded qubits.

When a teleportation gate fails it does so by making a measurement of an incoming qubit. This is always heralded and can be fixed using detected-measurement codes. This enables the scheme to be scalable (i.e. fault-tolerant) provided the intrinsic error probability is <0.5,[1] but at the expense of very complicated, multi-mode, entangled, resource states for teleportation. The other major source of error is photon loss. In principle, this can also be corrected using teleportation gates. Scalability requires that loss probability per gate be <0.01.[7] Not detecting a photon is equivalent to loss. While there are proposals for single-photon detectors that have quantum efficiency higher than 99%, using cycling transitions in atomic vapors,[8,9] currently the best known value is around 93%.[10]

Three experiments have implemented conditional two-qubit gates: Pittman et al.;[11] O'Brien et al.;[12] and Sanaka et al.[13] The first experiment is based on the Pittman and Franson's polarization-encoded scheme.[11] The second is based on a simplification of the KLM-NS gate that requires only two photons.[12] The last is a full four photon version of KLM.[13] However, all experiments so far only work in the coincidence basis. This means that successful implementations correspond to two- or four-fold coincidence counts. However, no light leaves the device as all photons are detected.

Experimental results obtained from a CNOT gate in Ref. 11 are shown in Fig. 4. Here, a single ancilla photon was used, which restricts the operation of the device to the case in which a single photon is detected in each output port (the so-called coincidence basis). This was a three-photon experiment in which two of the single photons were obtained using parametric down-conversion while the third photon was obtained by attenuating the pump laser beam. Optical fibres were used instead of free-space components in order to reduce errors due to mode mismatch. The fidelity of the output qubits was limited in this case by the degree of indistinguishability of the three photons. Experimental demonstrations of several other simple quantum logic gates have also been performed, including a quantum parity check[14] and a quantum encoder.[15]

2. REQUIREMENTS

There are four major technical requirements that must be met:

(1) Single photon sources
(2) Number-discriminating photon detectors
(3) Feed-forward control and quantum memory
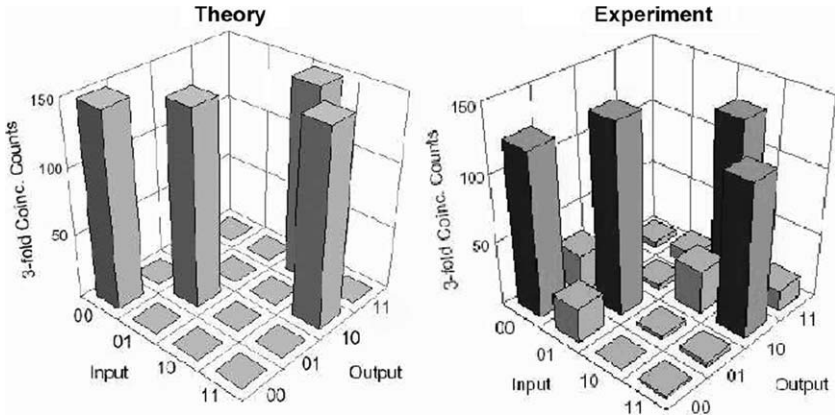(4) Design and implementation of the very complex quantum circuit architectures.

Fig. 4. Implementation of a probabilistic CNOT gate using polarization-encoded qubits.[11]

The required ideal single-photon sources are transform-limited pulses with one and only one photon per pulse. In practice, this means that one must be able to exhibit HOM interference between photons from different pulses. The required single-photon detectors must be able to detect a single photon with efficiency >0.99 and discriminate between 0, 1, and 2 photon counts.[16] Although two-photon interference visibilities >99% have been achieved,[11] it may be necessary to achieve even higher visibilities for quantum computing applications.

One approach to implementing such a single-photon source is illustrated in Fig. 5. A pulsed laser beam generates pairs of photons in a parametric down-conversion crystal. Detection of one member of a pair signals the presence of the other member of the pair, which is then switched into an optical storage loop. The single photon can then be switched out of the storage loop when needed.[18] Although this kind of approach cannot produce photons at arbitrary times, it can produce them at periodic time intervals that could be synchronized with the cycle time of a quantum computer. A prototype experiment of this kind demonstrated the ability to store and retrieve single photons in this way, but its performance at the time was limited by losses in the optical switch.

The ability to switch a single photon into an optical storage loop and then retrieve it when needed can also be used to implement a quantum memory for single photons. This application is more demanding than the single-photon source described above, since the polarization state of the photons must be maintained in order to preserve the value of the qubits. A prototype experiment of this kind has also been performed, where the primary limitation was once again the losses in the optical switch.[19]
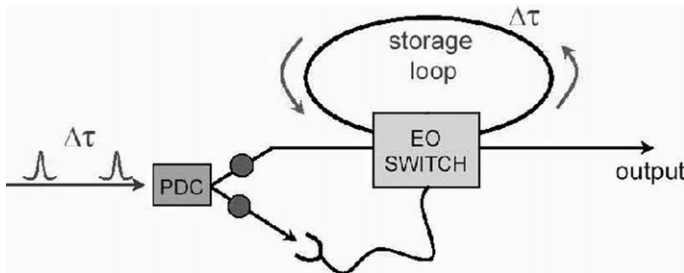
Fig. 5. Single-photon source using parametric down-conversion and an optical storage loop. Similar storage techniques can also be used to implement a quantum memory device for single photons.
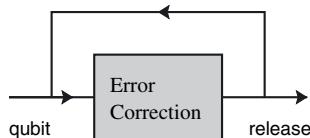

Fig. 6.   A cyclic quantum memory based on quantum error correction.

Furthermore, the ability to perform quantum logic operations using linear elements raises the possibility of using quantum error correction techniques to extend the coherent storage time of the quantum memory described above, see Fig. 6. The primary source of error is expected to be photon loss, which can be corrected using a simple four-qubit encoding scheme[20] as illustrated in Fig. 7. Provided that the errors in the logic gates and storage loops are sufficiently small, techniques of this kind can be used to store photonic qubits for an indefinitely long period of time.

An essential component in this kind of quantum memory is the single-photon quantum non-demolition (QND) measurement device.[21] Again, a simple way to perform a single-photon QND measurement is provided by quantum teleportation techniques. If the input state is in a arbitrary superposition of zero and one photon, with a fixed polarization, the detector coincidence in a Bell-state measurement signals the present of a single photon in the input and output states.[22]

Similar techniques can also be used to compensate for the photon loss in optical fibre transmission lines, which would allow the development of a quantum repeater. A quantum repeater is a device for achieving remote, shared entanglement by using quantum purification and swapping protocols.[23] A simple protocol for optical quantum repeaters based on linear optical elements and an entangled-photon source has been developed.[24] On the other hand, utilizing quantum error correction, one can relay an
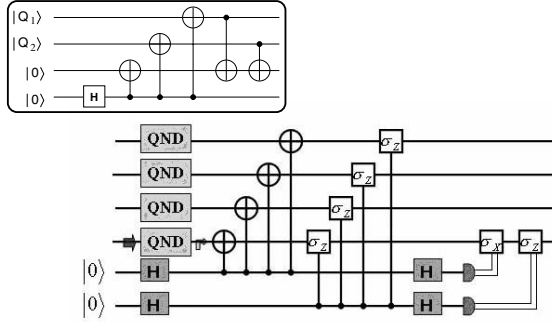
Fig. 7. Quantum error-correction code that recovers photon loss using two ancilla photons. The QND box represents a single-photon quantum non-demolition measurement device. The inset shows the two-to-four qubit encoding.

unknown quantum state with high fidelity down a quantum channel. This relay device we call a quantum transponder, and it has direct applications to quantum repeater and memory applications.

The fact that the LOQC architecture employs a non-deterministic protocol implies that large number of ancilla photons are required to make the scheme nearly deterministic. The implementation of quantum circuits then becomes more demanding with these increased number of resources. For example, implementing the error-correction circuit in Fig. 7 at $>80\%$ success probability requires more than 300 ancilla photons for each two-qubit gate and the same number of single-photon detections at the extremely high quantum efficiency.[20] Using a concatenation scheme to manage a single two-qubit gate with 95% success probability requires about 300 successful $CZ_{9/16}$ gate operations.[1] Therefore, development of techniques for efficient simplification of quantum circuits is an important task, as is the ability to fabricate these circuits on an opto-electonic chip.

On the other hand, QIP schemes implemented in unconventional ways, such as cluster state quantum computing,[25] may be utilized to reduce the number of resources. It has recently been shown that the required number of optical elements and resources can be reduced by an order of magnitude from the original KLM scheme by using multi photon-linked states,[26] and even more reduction has been found by using the cluster-state approach.[27] Furthermore, it may be possible to avoid the need for large number of nested interferometers and entangled ancillæ by using hybrid approaches that combine linear optics techniques with some amount of non-linearity.[28]

3. CONCLUSION

Quantum mechanics enables some exponentially more efficient algorithms than those that can be implemented on a classical computer. This discovery has led to the explosive growth of the field of quantum computation. Many physical systems have been suggested for building a quantum computer, but the final architecture is still to be determined. These systems include ion traps, non-linear optical systems, quantum dots, and superconducting circuits, among others.[29] In linear optical quantum computing the desired non-linearities come from projective measurements. Projective measurements over some part of the quantum system simply project the rest of the system into a desired quantum state. Additional photons, known as ancillæ, are mixed with the inputs to the logic devices using beam splitters, while single-photon detectors are used to make measurements on the ancilla photons after the interaction. The non-linear nature of single-photon detection and the quantum measurement process then project out the desired logical output. Therefore, although logic operations are inherently non-linear, our approach uses only simple linear optical elements, such as beam splitters and phase shifters. Building a quantum computer will be a major challenge for a future quantum technology; requiring the ability to manipulate quantum-entangled states of large number of sub components. Systematic development of each component of preparation, control, and measurement will facilitate the task of building a quantum computer.

ACKNOWLEDGMENTS

REFERENCES

1. E. Knill, R. Laflamme, and G. J. Milburn, *Nature* **409**, 46 (2001).
2. G. G. Lapaire, P. Kok, J. P. Dowling, and J. E. Sipe, *Phys. Rev. A* **68**, 042314 (2003).

3. T. B. Pittman, B. C. Jacobs, and J. D. Franson, *Phys. Rev. A* **64**, 062311 (2001).

4. T. B. Pittman, B. C. Jacobs, and J. D. Franson, *Phys. Rev. A* **66**, 052305 (2002).

5. D. Gottesman and I. L. Chuang, *Nature* **402**, 390 (1999).

6. J. D. Franson *et al.*, *Phys. Rev. Lett.* **89**, 137901 (2002).

7. E. Knill, R. Laflamme, and G. J. Milburn, quant-ph/0006120 (2000).

8. D. F. V. James and P. G. Kwiat, *Phys. Rev. Lett.* **89**, 183601 (2002).

9. A. Imamoglu, *Phys. Rev. Lett.* **89**, 163602 (2002).

10. E. Waks, *et al.*, *IEEE J. Sel. Top. Quant. Ele.* **9**, 1502 (2003).

11. T. B. Pittman, M. J. Fitch, B. C. Jacobs, and J. D. Franson, *Phys. Rev. A* **68**, 032316 (2003).

12. J. L. O'Brien *et al.*, *Nature* **426**, 264 (2003).

13. K. Sanaka *et al.*, *Phys. Rev. Lett.* **92**, 017902 (2004).

14. T. B. Pittman, B. C. Jacobs, and J. D. Franson, *Phys. Rev. Lett.* **88**, 257902 (2002).

15. T. B. Pittman, B. C. Jacobs, and J. D. Franson, *Phys. Rev. Lett. A* **69**, 042306 (2004).

16. D. Achilles *et al.* (in press) *J. Mod. Opt.* quant-ph/0310183 (2003); H. Lee *et al.*, *J. Mod. Opt.*, quant-ph/0310161 (2003).

17. T. B. Pittman and J. D. Franson, *Phys. Rev. Lett.* **90**, 240401 (2003).

18. T. B. Pittman, B. C. Jacobs, and J. D. Franson, *Phys. Rev. A* **66**, 042303 (2002).

19. T. B. Pittman and J. D. Franson, *Phys. Rev. A* **66**, 062302 (2002).

20. R. M. Gingrich *et al.*, *Phys. Rev. Lett.* **91**, 217901 (2003).

21. G. Nogues *et al.*, *Nature* **400**, 239 (1999).

22. P. Kok, H. Lee, and J. P. Dowling, *Phys. Rev. A* **66**, 063814 (2002).

23. H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **81**, 5932 (1998).

24. P. Kok, C. P. Williams, and J. P. Dowling, *Phys. Rev. A* **68**, 022301 (2003).

25. R. Raussendorf and H.-J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).

26. N. Yoran and B. Reznik, *Phys. Rev. Lett.* **91**, 037903 (2003).

27. M. Nielsen, quant-ph/0402005 (2004).

28. J. D. Franson, T. B. Pittman, and B. C. Jacobs, quant-ph/0401133 (2004).

29. J. P. Dowling and G. J. Milburn, *Phil. Trans. R. Soc. Lond. A* **361**, 1655 (2003).