Quantum Information and Computation, Vol. 1, Special Issue (2001) 13–19
© Rinton Press

EFFICIENT LINEAR OPTICS QUANTUM COPUTATION

G. J. Milburn[1], T.Ralph[1], A. White[1], E. Knill[2], and R. Laflamme[2]

[1] *Centre for Quantum Computer Technology, Univ. of Queensland, St. Lucia, Australia*

[2] *Los Alamos National Laboratory, MS B265, Los Alamos, NM 87545, USA*

Two qubit gates for photons are generally thought to require exotic materials with huge optical nonlinearities. We show here that, if we accept two qubit gates that only work conditionally, single photon sources, passive linear optics and particle detectors are sufficient for implementing reliable quantum algorithms. The conditional nature of the gates requires feed-forward from the detectors to the optical elements. Without feed forward, non-deterministic quantum computation is possible. We discuss one proposed single photon source based on the surface acoustic wave guiding of single electrons.

One of the earliest proposals [1] for implementing quantum computation was based on encoding each qubit in two optical modes together containing exactly one photon. However it is extremely difficult to unitarily couple two optical modes containing few photons. Here we consider the question of what can be achieved in principle using combinations of only the simplest optical elements: passive linear optics, photodetectors, and single photon sources.

The dynamics implemented by passive linear optics conserves the total number of bosons in the modes. It is therefore convenient to describe them by their effect on the creation operators. Specifically, if U is the unitary operator associated with the evolution, then U takes the state ${\mathbf{a}^{(l)}}^\dagger|\mathbf{0}\rangle$ to

$$\begin{aligned} U{\mathbf{a}^{(l)}}^\dagger|\mathbf{0}\rangle &= U{\mathbf{a}^{(l)}}^\dagger U^\dagger|\mathbf{0}\rangle &(1)\\ &= \sum_m U_{ml}{\mathbf{a}^{(m)}}^\dagger|\mathbf{0}\rangle, &(2)\end{aligned}$$

using the fact that $U^\dagger|\mathbf{0}\rangle = |\mathbf{0}\rangle$. The matrix defined by the coefficients U_{ml} must be unitary, and furthermore, for all unitary U_{ml}, there is a sequence of phase shifter and beam splitter evolutions which implements the corresponding operation [2]. For a named optical element X, let $U(X)$ be the unitary matrix associated with X according to the above rules. The unitary matrices associated with phase shifters ${P_\theta}^{(l)}$ and beam splitters ${B_\theta}^{(lm)}$ are:

$$\begin{aligned} U({P_\theta}^{(1)}) &= e^{i\theta}\\ U({B_\theta}^{(12)}) &= \begin{pmatrix} \cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{pmatrix}.\end{aligned}$$

General linear optical elements have Hamiltonians which consist of terms at most quadratic in the annihilation and creation operators.

We choose the traditional encoding of photonic qubits based on a "dual rail" logic, using two modes and one photon;

$$\begin{aligned} |0\rangle_L &= |1\rangle_1 \otimes |0\rangle_2 &(3)\\ |1\rangle_L &= |0\rangle_1 \otimes |1\rangle_2 \quad . &(4)\end{aligned}$$

The modes could be two input modes to a beam splitter distinguished by the different directions of the wave vector, or they could be distinguished by polarisation. In the case of a beam splitter a single qubit gate is easily implemented by the linear transformation

$$a_i(\theta) = U(\theta)^\dagger a_i U(\theta) \tag{5}$$

with $U_{12}(\theta) = \exp\left[i\theta(a_1^\dagger a_2 + a_1 a_2^\dagger)\right]$. Thus

$$\begin{aligned} a_1(\theta) &= \cos\theta a_1 - i\sin\theta a_2 \\ a_2(\theta) &= \cos\theta a_2 - i\sin\theta a_1 \end{aligned}$$

The description in the logical basis becomes,

$$|0\rangle_L \to \cos\theta_1|0\rangle_L - i\sin\theta_1|1\rangle_L \tag{6}$$

In addition to a single qubit gate, universal quantum computation requires at least a two qubit gate. A simple choice is the conditional sign shift gate,

$$|x\rangle_L|y\rangle_L \to e^{i\pi x.y}|x\rangle_L|y\rangle_L \tag{7}$$

Unfortunately this is difficult to implement with the optical qubits as photons do not interact except via matter. The mutual Kerr nonlinear phase shift is one such interaction,

$$U_{NL} = \exp[i\pi a_1^\dagger a_1 a_2^\dagger a_2] \tag{8}$$

In practice it is not possible to get a single photon phase shift of π, which this transformation implies, without adding a considerable amount of noise from the electronic systems that mediate the interaction. However, as we now show, we can get an effective nonlinear sign shift with linear optical transformations, such as a beam splitter, by coupling the modes of interest to ancilla modes and performing single photon detection on these ancilla modes. Under the right circumstances the conditional states corresponding to observed counts at the ancilla modes will effect the required conditional phase shift.

We first give a simple illustration of the principle. Suppose we mix two modes at a beam splitter and count photons only on one output mode, say mode a_2. We will assume that mode a_2 is initially in the vacuum state. The conditional state of mode a_1, given a count n is given by

$$|\psi^{(n)}\rangle_1 = \hat{E}_n|\psi\rangle_1 \tag{9}$$

where $|\psi\rangle_1$ is the input state for mode a_1 and the measurement operator is

$$\hat{E}_n = {}_2\langle n|U(\theta)|0\rangle_2. \tag{10}$$

The case of interest here, where $n = 0, 1$, is given by

$$\begin{aligned} \hat{E}_0 &= \sum_{n=0}^{\infty} \frac{(\cos\theta - 1)^n}{n!}(a_1^\dagger)^n a_1^n & (11) \\ \hat{E}_1 &= \cos\theta\hat{E}_0 - \sin^2\theta a_1^\dagger \hat{E}_0 a_1 & (12) \end{aligned}$$

In this way a simple beam splitter can implement a conditional phase shift for a particular number state in mode a_1.

We seek to implement the conditional nonlinear sign shift for the state of mode a_1 defined by,

$$|\phi\rangle = \alpha_0|0\rangle_0 + \alpha_1|1\rangle_1 + \alpha_2|2\rangle_1 \to \alpha_0|0\rangle_1 + \alpha_1|1\rangle_1 - \alpha_2|2\rangle_1 \tag{13}$$

We use two ancilla modes, a_2, a_3 which can be regarded as a representing a single qubit in dual rail logic: $|0\rangle_L = |1\rangle_2|0\rangle_3 \quad |1\rangle_L = |0\rangle_2|1\rangle_3$ In the *first step*, single qubit rotation is performed on modes $2-3$, prepared in state $|0\rangle_L$, with the unitary operator $U_{23}(\theta_1)$,

$$|0\rangle_L \to \cos\theta_1|0\rangle_L - i\sin\theta_1|1\rangle_L \tag{14}$$

In the *second step*, mode a_2 of this qubit is coupled to the signal mode,

$$U_{12}(\theta_2)\left[\cos\theta_1|0\rangle_L - i\sin\theta_1|1\rangle_L\right]|\psi\rangle_1 \qquad (15)$$

where $|\psi\rangle_1$ is the signal input state. In the *third step* a final qubit rotation through an angle θ_3 is again performed on modes a_2, a_3 with the unitary $U_{23}(\theta_3)$, and a photon counter records a count on each of the qubit modes. We will show that the conditional sign shift is implemented when the count is $n_2 = 1,\ n_3 = 0$. This corresponds to projecting out the logical state $|0\rangle_L$ on the qubit in modes a_2, a_3.

The corresponding conditional state is then seen to be,

$$|\psi^{(0)}\rangle_1 = \cos\theta_1\cos\theta_3\hat{E}^{(1)}(\theta_2)|\psi\rangle_1 - \sin\theta_1\sin\theta_3\hat{E}^{(0)}(\theta_2)|\psi\rangle_1 \qquad (16)$$

For the desired conditional nonlinear sign shift gate (NS gate) we require,

$$\begin{aligned} \cos\theta_1\cos\theta_3\cos\theta_2 - \sin\theta_1\sin\theta_3 &= \lambda \\ \cos\theta_1\cos\theta_3\cos 2\theta_2 - \sin\theta_1\sin\theta_3\cos\theta_2 &= \lambda \\ \cos\theta_1\cos\theta_3\cos\theta_2(\cos^2\theta_2 - 2\sin^2\theta_2) - \sin\theta_1\sin\theta_3\cos^2\theta_2 &= -\lambda \end{aligned}$$

The solution is easily seen to be $\theta_1 = \theta_2 = 22.5^o \quad \theta_2 = 114.47^o$ with $\lambda = -1/2$. The success probability is $\lambda^2 = 1/4$.

In figure 1 we show how two non deterministic NS gates can be used to implement a two qubit conditional NOT gate, a CNOT gate. We employ dual rail logic such that the "control in" qubit is represented by the two bosonic mode operators c_H and c_V. A single photon occupation of c_H with c_V in a vacuum state will be our logical 0, which we will write $|H\rangle$ (to avoid confusion with the vacuum state). Whilst a single photon occupation of c_V with c_H in a vacuum state will be our logical 1, which we will write $|V\rangle$. Of course superposition states can also be formed. Similarly the "target in" is represented by the bosonic mode operators t_H and t_V with the same interpretations as for the control. The beamsplitters, $B1$, $B2$, $B3$ and $B4$ are all 50:50. The use of the "H", "V" nomenclature alludes to the standard situation in which the two modes of the dual rail logic are orthogonal polarisation modes. Conversion of a polarisation qubit into the spatial encoding used to implement the CNOT gate can be achieved experimentally by passing the photon through a polarising beamsplitter, to spatially separate the modes, and then using a half-wave plate to rotate one of the modes into the same polarisation as the other. After the gate, the reverse process can be used to return the encoding to polarisation. As success requires the two NS gates to work the overall probability of success is 1/16.

The layout of figure 1 contains two nested, balanced Mach-Zehnder interferometers. The target modes are combined and then re-separated forming the "T"interferometer. One arm of the T interferometer and the c_V mode of the control are combined to form another interferometer, the "C" interferometer. NS gates are placed in both arms of the C interferometer. The essential feature of the system is that if the control photon is in the c_H mode then there is never more that one photon in the C interferometer, so the NS gates do not produce a change, the T interferometer remains balanced and the target qubits exit in the same spatial modes in which they entered. On the other hand if the control photon is in mode c_V then there is a two photon component in the C interferometer which suffers a sign change due to the NS gates. This leads to a sign change in one arm of the T interferometer and the target qubit exits from the opposite mode from which it entered.

The CNOT gate previously described can be considerably simplified at the expense of a small decrease in success probability. A major simplification is achieved by operating the NS gates in a biased mode. The idea is to set the parameters θ_1 and θ_3 in the NS gates to zero, i.e. the beam splitters are totally reflective. This removes the interferometers from both the NS gates, greatly reducing the complexity of the gate. Summing over the paths as before we find that the NS operation becomes

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \rightarrow |\psi'\rangle = \sqrt{\eta_2}\alpha|0\rangle + (1-2\eta_2)\beta|1\rangle - \sqrt{\eta_2}(2-3\eta_2)\gamma|2\rangle \qquad (17)$$

when $\theta_1 = \theta_3 = 0$ and we have put $\eta_2 = \cos\theta_2$. There is no solution such that the "0", "1" and "2" components scale equally, so the gate is biased. As a result it is not possible

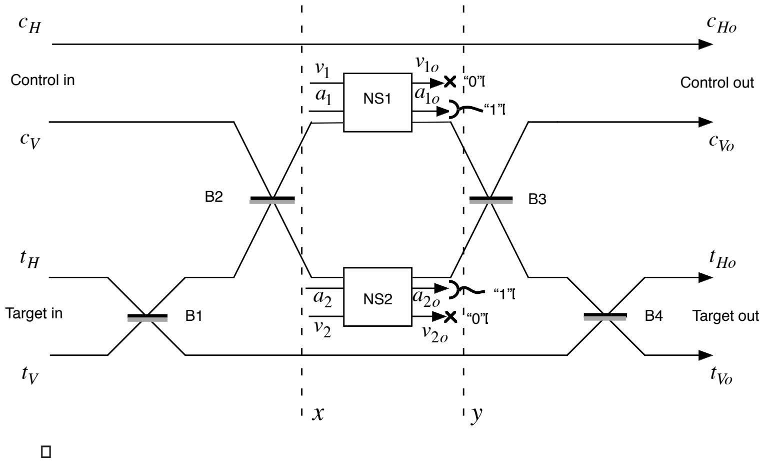

Fig. 1. A CNOT two qubit gate implemented using two non deterministic nonlinear sign shift gates.

to pick an η_2 such that the T interferometer is simultaneously balanced for both the case of a photon in c_{Ho} and the case of a photon in c_{Vo}. This problem can be solved by including some additional attenuation. One of a number of possible scenarios is shown in figure 2. The NS gates have been replaced by the beamsplitters B5 and B6 which have reflectivities η_2. Additional beamsplitters, B7 and B8, of refectivities η_7 have been inserted in beams c_V and t' respectively. The state of the system at point z in figure 2 (conditional on a single photon being detected at outputs a_{1o} and a_{2o} *and* no photons appearing at outputs v_{7o} and v_{8o}) is given by

$$|\psi\rangle_y = \frac{1}{\sqrt{2}}\eta_2|1001\rangle \pm \sqrt{\eta_2\eta_7}(1-2\eta_2)\frac{1}{2}(|1100\rangle - |1010\rangle) \qquad (18)$$

if the control is initially in $|H\rangle$ and

$$|\psi\rangle_y = \frac{1}{2}(\sqrt{\eta_2\eta_7}(1-2\eta_2)(|0101\rangle + |0011\rangle) \mp (\eta_7\eta_2(2-3\eta_2)(|0200\rangle - |0020\rangle))) \qquad (19)$$

if the control is initially in $|V\rangle$. It is now possible to simultaneously balance the T interferometer for both inputs by choosing $\eta_2 = (3-\sqrt{2})/7$ and $\eta_7 = 5 - 3\sqrt{2}$. CNOT operation then occurs with a probability $\eta_2^2 \approx 0.05$. All the conditional moments of the original CNOT gate are reproduced but with the probabilities of the non-zero moments reduced from 1/16 to approximately 1/20. All other properties of the original gate are retained.

A cascaded sequence of non deterministic gates is useless for quantum computation as the probability of many gates working in sequence would decrease exponentially. We now show how to avoid this by using a teleportation protocol to only implement a gate in a quantum circuit if it works. In essence we hold back the gate until we are sure it works and then teleport it onto the required stage of the computation. The idea that teleportation can be used for universal quantum computation was first proposed by Gottesman and Chuang [3]. The idea is to prepare a suitable entangled state for a teleportation protocol with the required gate already applied. We use a non deterministic NS gate to prepare the required entangled state, and only complete the teleportation when the this stage is known to work. The teleportation step itself is non deterministic, but we will show that by using the appropriate entangled resource the teleportation step can be made near deterministic. The near deterministic teleportation protocol requires only photon counting and fast feedforward. We do not need to make measurements in a Bell basis.

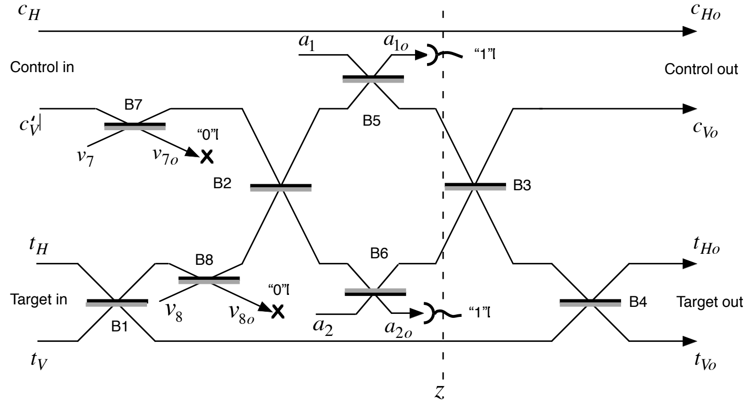

Fig. 2. A simplified CNOT two qubit gate.

A basic quantum teleportation protocol for transferring the state $\alpha_0|0\rangle_0 + \alpha_1|1\rangle_0$ to mode 3 begins with adjoining the "entangled" ancilla state $|t_1\rangle_{12} = |01\rangle_{12} + |10\rangle_{12}$ to mode 1. (We omit normalisation constants wherever possible.) Note that in this case, the ancilla state is easily generated from $|10\rangle_{12}$ by means of a beam splitter.

The second step is to measure modes 0 and 1 in the basis $|01\rangle_{01} \pm |10\rangle_{01}, |00\rangle_{01} \pm |11\rangle_{01}$ (the "Bell basis"). We decompose the measurement into two steps. The first step determines the parity p of the number of bosons in modes 0 and 1 ("parity measurement"). The second determines the sign s in the superposition. Consider the case where $p = 1$. Then if $s =$ '+', the state of mode 2 is $\alpha_0|0\rangle_2 + \alpha_1|1\rangle_2$. If $s =$ '-', the state is $\alpha_0|0\rangle_2 - \alpha_1|1\rangle_2$, which can be restored to the starting state by using a phase shifter. For $p = 0$, the situation is similar except that $|0\rangle_2$ and $|1\rangle_2$ are flipped (and cannot be easily un-flipped using linear optics). The key property of quantum teleportation is that the input state appears in mode 2 up to a simple transformation without having interacted with mode 2 after the preparation of the initial ancilla state.

Consider the parity measurement. Applying a balanced beam splitter to modes 0 and 1 and then measuring the number of photons in the two modes successfully determines the parity, and if it is odd, the sign. As a result, it can be used to perform the teleportation with success probability 1/2. We refer to the partial Bell-state measurement as $\mathbf{BM}_1$ and to the corresponding teleportation protocol as $\mathbf{T}_{1/2}$.

The next step is to use $\mathbf{T}_{1/2}$ to design a conditional sign flip c-$\sigma_{z1/4}$ which succeeds with probability 1/4. To see how to do this, observe that to implement c-σ_z on two bosonic qubits in modes $1, 2$ and $3, 4$ respectively, we could try to first teleport the first modes of each qubit to two new modes (labelled 6 and 8) and then apply c-σ_z to the new modes. When using $\mathbf{T}_{1/2}$, we may need to apply a sign correction. Since this commutes with c-σ_z, there is nothing preventing us from applying c-σ_z to the prepared state before performing the measurements. The implementation is shown in Fig. 3 and now consists of first trying to prepare two copies of $|t_1\rangle$ with c-σ_z already applied, and then performing two $\mathbf{BM}_1$ measurements. Given the prepared state, the probability of success is $(1/2)^2$. The state can be prepared using c-$\sigma_{z1/16}$, which means that the preparation has to be retried an average of 16 times before it is possible to proceed.

To improve the probability of successful teleportation to $1 - 1/(n + 1)$, we generalise the

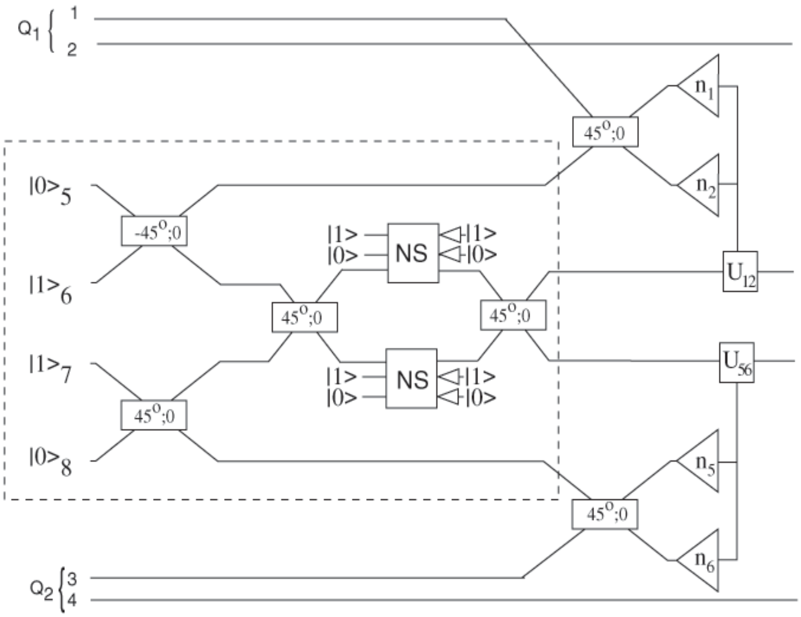

Fig. 3. A c-sign two qubit gate with teleportation to increase success probability to 1/4.

initial entanglement by defining

$$|\mathrm{t_n}\rangle_{1\ldots(2n)} = \sum_{j=0}^{n} |1\rangle^j|0\rangle^{n-j}|0\rangle^j|1\rangle^{n-j}. \tag{20}$$

The notation $|a\rangle^j$ means $|a\rangle|a\rangle\ldots$, j times. The modes are labelled from 1 to $2n$, left to right. Note that the state exists in the space of n bosonic qubits, where the k'th qubit is encoded in modes $n+k$ and k (in this order).

To teleport the state $\alpha_0|0\rangle_0 + \alpha_1|1\rangle_0$ using $|\mathrm{t_n}\rangle$ use the measurement $\mathbf{BM}_n$ implemented by first applying an $n+1$ point Fourier transform $\hat{\mathbf{F}}_{n+1}$ on modes 0 to n. $\hat{\mathbf{F}}_{n+1}$ is defined by

$$u(\hat{\mathbf{F}}_{n+1})_{kl} = \omega^{kl}/\sqrt{n+1}, \tag{21}$$

where $\omega = e^{i2\pi/(n+1)}$ and $k, l \in 0\ldots n$. It is by definition implementable with passive linear optics. Using the parallel fast Fourier transform (see page 795 of [4]), it can be implemented with $O(n\log(n))$ elements and depth $O(\log(n))$, for n a power of 2. Alternatively, a multiport generalisation of the Mach-Zehnder interferometer can be used [5]. After applying $\hat{\mathbf{F}}_{n+1}$, $\mathbf{BM}_n$ measures the number of photons in each of the modes 0 to n.

Suppose $\mathbf{BM}_n$ detects k bosons altogether. It is possible to show [6] that if $0 < k < n+1$, then the teleported state appears in mode $n+k$ and only needs to be corrected by applying a phase shift. The modes $2n-l$ are in state 1 for $0 \le l < (n-k)$ and can be reused in future preparations requiring single bosons. The modes are in state 0 for $n-k < l < n$. If $k=0$ we learn that the input state is measured and projected to $|0\rangle_0$ and if $k = n+1$, it is projected to $|1\rangle_0$. The probability of these two events is $1/(n+1)$, regardless of the input. We will make use of the fact that failure is detected and corresponds to measurements in the basis $|0\rangle, |1\rangle$ with the outcome known. Note that both the necessary correction and which mode we teleported to are unknown until after the measurement.

There are two problems with the methods shown so far. The first is that for large n, the obvious networks for preparing the required states have very low probabilities of success. It is therefore desirable to avoid using the methods with large n. The second problem is that to get decent success probabilities for coupling gates does large n, particularly if it is necessary to meet the accuracy requirements of reliable quantum computing.

To achieve exponential improvements in the probability of success for gates and state production with small n, we use quantum codes and exploit the properties of the failure behaviour of c-$\sigma_{zn^2/(n+1)^2}$. For details see Knill et al. [6]. As a result it is possible to iterate the methods to efficiently achieve essentially perfect quantum computation. This iteration is known as *concatenation* and underlies the accuracy threshold theorems of fault tolerant quantum computation [7, 8, 9, 10].

To conclude we summarise the physical requirements for linear optics quantum computation. The Scheme requires: (i) single photon sources (ii) fast efficient single photon detectors, (iii) low photon absorption and (iv) fast electro-optics feed forward. There is currently a great deal of interest in schemes for single photon sources[11] and recently a particularly useful scheme was demonstrated.We expect that reliable and fast single photon sources are not far away. In the mean time however the basic elements of linear optics QC could be demonstrated with conditional non deterministic single photon sources, such as are used in parametric down conversion experiments[12]. The requirement for fast single photon detectors that can distinguish zero, one and two photons is a difficult one to meet with current technology, but is achievable by a variety of means. Low photon absorption is not in principle a problem. As was demonstrated by Knill et al.[6], there are linear optics protocols that can detect for photon loss. The requirement of fast electro optic feed forward is perhaps the biggest hurdle to overcome for demonstrating a simple quantum circuit. The near deterministic teleportation steps require some kind of delay line before measurement results are fed forward. This places strong bandwidth requirements on any electro-optical processes. Despite these difficulties we expect that the basic elements of linear optics quantum computation will be demonstrated in the next few years and in the long run reliable linear optics quantum computation may be no more difficult than other schemes for large scale quantum computation.

References

1. G.J.Milburn, Phys. Rev. Lett. **62**, 2124–2127 (1988).
2. M. Reck, A.Zeilinger, H. J.Bernstein, and P.Bertani, Phys. Rev. Lett., **73**, 58–61 (1994).
3. D.Gottesman, and I.L.Chuang, Nature, **402**, 390–393 (1999).
4. T.H.Cormen, C.E.Leiserson, and R.L.Rivest, *Introduction to Algorithms*, MIT Press, Cambridge, Mass, (1990).
5. G.Weihs, M.Reck, H.Weinfurter, and A.Zeilinger, Opt. Lett. **21**, 302–304 (1996).
6. E.Knill,R.Laflamme and G.J.Milburn, Nature, **409**, 46, (2001).
7. D.Aharonov, and M. Ben-Or, In *Proceedings of the 29th Annual ACM Symposium on the Theory of Computation (STOC)*, 176–188 (ACM Press, New York, New York, 1996).
8. A.Y.Kitaev, Quantum computations: algorithms and error correction. Uspekhi Mat. Nauk. **52**, 53–112 (1997).
9. E.Knill, R.Laflamme, and W.H.Zurek, Science, **279**, 342–345 (1998).
10. J.Preskill, Proc. R. Soc. Lond. A, **454**, 385–410 (1998).
11. C.Foden,V.I.Talyanskii,G.J.Milburn,M.L.Leadbeater, and M. Pepper, Phys. Rev. A, **62**, 011803(R), 1-4(2000).
12. D.Bouwmeester, J.-W.Pan, M.Daniell,H.Weinfurter,A.Zeilinger, Phys. Rev. Lett. **82**, 1345, (1999).