Linear Optics Quantum Computation

Jacob Marttinen
20313145 - CS467
University of Waterloo

January 16, 2013

Abstract

Numerous possible implementations have been proposed for quantum computers, but there is no clear best implementation at this point in time. One possibility is linear optical quantum computing. As with every proposed implementation, optical quantum computing has its own strengths and weaknesses.

Throughout this paper, we will discuss the fundamental requirements for an optical quantum computer and the groundbreaking KLM (Knill, Laflamme, and Milburn) proposal, as well as resultant improvements and suggestions. The possible errors related to realistic physical optical components are summarized, along with schemes for error correction to overcome these inevitable errors. Finally we briefly touch on the future of linear optical quantum computing.

1 Introduction to Optical Quantum Computing

Quantum computing has attracted a lot of attention in the scientific community over the past 15-20 years, largely due to its promise for super fast factoring and the efficient simulation of quantum dynamics. During this time, there have been a number of proposed possibilities for implementing quantum computers; these include atom- and ion-trap quantum computing, superconducting charge and flux qubits, nuclear magnetic resonance, spin- and charge-based quantum dots, nuclear spin quantum computing, and optical quantum computing (OQC) [9]. However, as the quantum computing field is still in its infancy, there is no clear best implementation for a quantum computer.

Although each of the listed possibilities has its own strengths and weaknesses, OQC has the advantage of having the smallest unit of quantum information (the photon). Although photons are characteristically free from decoherence (quantum information stored in a photon tends to stay there), they do not naturally interact with each other [6]. In order to apply two-qubit quantum gates, such photon interactions are essential. In this paper, we discuss linear optics as a method of implementing OQC.

An optical circuit can be thought of using a black box model with both incoming and outgoing streams of photons. This black box transforms a state of the incoming streams into the (different state of the) outgoing streams. Beam splitters might mix the streams of photons, or they may pick up a relative phase shift or polarization rotation. As this black box model can be considered perfect, these operations preserve the photon number (number of photons in the stream). In addition, the box may include measurement devices, the outcomes of which may modify optical components on the remaining modes. This continuous modification is called feed-forward detection, and it is an important technique that can increase the efficiency of a device [6].

Such a black box model can be implemented using the basic building blocks of linear optics: beam splitters, half- and quarter-wave plates, phase shifters, etc. Semi-reflective mirrors can physically represent beam splitters: when light falls on this mirror, part will be reflected and part will be transmitted. Half- and quarter-wave plates are used to apply polarization rotation to qubits. Physically, a phase shifter can be pictured as a slab of transparent material with an index of refraction that is different from that of free space. Other building blocks of linear optics exist, but these form the core of the current proposals for the implementation of linear OQC.

For any implementation of a quantum computer, we need some way to represent a qubit. In linear OQC, a qubit is usually taken to be a single photon that has the choice of two different modes [6]:

$$|0\rangle_L = |1\rangle \otimes |0\rangle \equiv |1,0\rangle \text{ and } |1\rangle_L = |0\rangle \otimes |1\rangle \equiv |0,1\rangle$$

Such a photon is called a dual-rail qubit. When the two modes represent the internal polarization degree of freedom of the photon ($|0\rangle_L = |H\rangle$ and $|1\rangle_L = |V\rangle$), the photon is referred to as a polarization qubit. These two representations are mathematically equivalent, and we can physically switch between them using polarization beam splitters [8].

As seen in lecture, we need both single-qubit operations as well as two-qubit operations to build a quantum computer [1]. Single-qubit operations are generated by the Pauli operators, which represent a rotation about the Bloch sphere. These operations can be implemented with phase shifters, beam splitters, and polarization rotations on polarization and dual-rail qubits. While single-qubit operations can be implemented in a straightforward fashion, two-qubit gates in linear OQC are more problematic. However, we need at least a single two-qubit gate to implement a deterministic universal quantum gate set. Another major difficulty with implementing linear OQC is that the obvious methods of defining gates probabilistically result in failure more often than not. As such failures typically destroy the associated quantum information in the process, optical quantum gates must be nonprobabilistic [6]. To work around these (and other) initial difficulties, two main physical architectures for implementing linear OQC have been proposed: the KLM architecture (proposed by Knill, Laflamme, and Milburn in 2001 [4]) and the one-way quantum computer with cluster states (proposed by Raussendorf and Briegel in 2001 [8]).

2 Optical Quantum Computing Paradigm

In 2000, Knill, Laflamme, and Milburn proved that it is indeed possible to create universal quantum computers with linear optics, single photons, and photon detection [4]. They constructed an explicit protocol involving off-line resources, quantum teleportation, and error correction. However, we first need to discuss a number of fundamental requirements for OQC before we get into this proposal.

2.1 Fundamental Requirements

Physically, the reason why we cannot construct deterministic (nonprobabilistic) two-qubit gates in either the polarization or the dual-rail representations is that photons do not naturally interact with each other. The only way in which photons can directly influence each other is via the bosonic symmetry relation [6]. (In a theory with the existence of supersymmetry, for every type of boson there exists a corresponding type of fermion with the same mass and internal quantum numbers, and vice-versa.) Linear OQC utilizes exactly this property. Essentially, when two identical single-photon wave packets enter a 50:50 beam splitter (one in each input mode) with a perfect temporal overlap, the two photons will always exit the beam splitter together in the same output mode (with a 50:50 chance of exiting either output mode). This is known as the Hong-Ou-Mandel effect (1987) [3]. However, this photon relation is not enough to make a deterministic linear OQC, and we must

$Control$	$Target$	CZ	$CNOT$
$\|0\rangle$	$\|0\rangle$	$\|0,0\rangle$	$\|0,0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0,1\rangle$	$\|0,1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1,0\rangle$	$\|1,1\rangle$
$\|1\rangle$	$\|1\rangle$	$-\|1,1\rangle$	$\|1,0\rangle$

Figure 1: The effects of the CZ and CNOT gates.

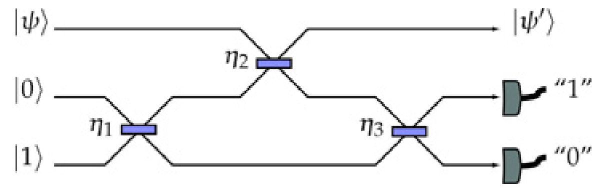

Figure 2: A nonlinear sign (NS) gate, as proposed by KLM [4].

instead turn our attention to probabilistic gates. This thinking is known to be physically feasible, as a number of experimental groups have already demonstrated all-optical probabilistic quantum gates.

In linear optics, we usually use the set {CZ, CNOT} (in addition to single-qubit gates) as our universal quantum gate set. The CZ gate is the controlled-phase gate, and the CNOT gate is the controlled-not gate [6]. Their effects are summarized in the truth table in Figure 1. A CZ gate can be constructed in linear optics using two NS (nonlinear sign) gates. The method of implementing an NS gate as proposed by KLM is shown in Figure 2 [4]. It should be clear that we could not make an NS gate with a regular phase shifter. However, we can perform the NS-gate probabilistically using projective measurements. The probability of success for such a probabilistic NS gate has an upper-bound probability of $\frac{1}{2}$, with a limit of $\frac{1}{4}$ without any feed-forward mechanism [4].

Another important gate is the parity check gate. This gate consists of a single polarizing beam splitter, followed by photon detection in the complementary basis of one output mode. The parity check gate induces the following transformation [8]:

$$\begin{array}{rcl} |H,H\rangle_{ab} & \rightarrow & |H,H\rangle_{cd'} \\ |H,V\rangle_{ab} & \rightarrow & |HV,0\rangle_{cd'} \\ |V,H\rangle_{ab} & \rightarrow & |0,HV\rangle_{cd'} \\ |V,V\rangle_{ab} & \rightarrow & |V,V\rangle_{cd'} \end{array}$$

Although we do not further discuss the usage of this gate, it is worth mentioning as it is used in a number of alternative modifications to the KLM protocol.

All the gates discussed so far are probabilistic, and indeed all two-qubit gates based on projective measurements must be probabilistic. Although it is possible (in principle) that feed-forward protocols can increase the probability of success, Knill demonstrated that the highest possible success probability for the NS gate (using feed-forward principles) is $\frac{1}{2}$ [5]. However, this bound is not tight, and numerical evidence strongly suggests an upper bound of $\frac{1}{3}$ for infinite feed-forward without entangled ancilla bits [6]. This tells us that the benefit of feed-forward may not outweigh its cost.

When the gates in a computational circuit succeed only with a certain probability p then the entire calculation that uses N such gates succeeds with probability p^N. For large N and small

p, this probability is miniscule. As a result of this low probability, we either have to repeat the calculation p^{-N} times or run p^{-N} such systems in parallel in order to achieve success. Either way, the resources (time or circuits) scale exponentially with the number of gates. Any advantage that quantum algorithms might have over classical algorithms quickly disappears when we consider the number of retrials or the amount of hardware we might need. In order to do useful computing with probabilistic gates, we have to take the probabilistic elements out of the running calculation. Gottesman and Chuang proposed a trick in 1999 that removes the probabilistic gate from the quantum circuit and places it in a set of resources that can be prepared offline. This trick is commonly referred to as the teleportation trick, since it "teleports the gate into the quantum circuit." [2]

Another issue to consider is the fact that quantum gates destroy the input qubits if the operation fails. Suppose we need to apply a probabilistic CZ gate to two qubits with quantum states $|\phi_1\rangle$ and $|\phi_2\rangle$. If we apply the gate directly to the qubits, we are very likely to destroy the qubits. However, suppose that we teleport both qubits from their initial mode to a different mode. There are now no longer any probabilistic elements in the computational circuit. It also may be sufficient on occasion to apply destructive two-photon gates. For example, a Bell measurement in teleportation does not need to be non-destructive in order to successfully teleport a photon. We can use this information to increase the probability of success of the gate considerably [4].

2.2 KLM Scheme

The KLM protocol was initially designed as a proof that linear optics and projective measurements can allow for scalable quantum computing in principle. However, it ended up subsequently inspiring numerous new experiments in quantum optics, demonstrating the feasible operation of high-fidelity probabilistic two-photon gates. The work by KLM was based on the important findings of Gottesman, Chuang, and Nielsen concerning the role of teleportation for universal quantum computing [2]. The basic idea of the KLM scheme is the teleportation of probabilistic two-photon gates into quantum circuits with high probability. Subsequent error correction in the quantum circuit is then used to bring the error rate down to fault tolerant levels. The physical resources for universal (optical) quantum computation in the KLM scheme are multi-particle entangled states and (entangling) multi-particle projective measurements. This allows for universal and scalable OQC using only single photons, linear optics, and measurement [4].

Unfortunately, there is a problem with our aforementioned teleportation trick when applied to linear optics: in our qubit representation, the Bell measurement (which is essential to quantum teleportation) is not complete and works at best only half of the time. This is one of the problems of linear OQC that was solved by KLM. In the KLM scheme, the qubits are chosen from the dual-rail representation. However, in the KLM protocol the teleportation trick applies to the single rail state $\alpha|0\rangle + \beta|1\rangle$. Linearity of quantum mechanics ensures that if we can teleport this state, we can also teleport any coherent or incoherent superposition of such a state [4]. We choose our quantum channel to be the $2n$-mode state:

$$|t_n\rangle = \frac{1}{\sqrt{n+1}} \textstyle\sum_{j=0}^{n} |1\rangle^j |0\rangle^{n-j} |0\rangle^j |1\rangle^{n-j} \text{ where } |k\rangle^j \equiv |k\rangle_1 \otimes ... \otimes |k\rangle_j$$

We can then teleport the state $\alpha|0\rangle + \beta|1\rangle$ by applying an $n+1$-point discrete quantum Fourier transform (QFT) to the input mode and the first n modes of $|t_n\rangle$. We then count the number of photons m in the output mode [4]. The discrete QFT F_n can be written in matrix notation as:

$$(F_n)_{jk} = \frac{1}{\sqrt{n}} exp\left[2\pi i \frac{(j-1)(k-1)}{n}\right]$$

F_n erases all path information of the incoming nodes, and can be interpreted as the n-mode generalization of the 50:50 beam splitter. Now that we have a (nearly) deterministic teleportation protocol, we have to apply the probabilistic gates to the auxiliary states $|t_n\rangle$ [4]. For the CZ gate, we need the auxiliary state:

$$|cz_n\rangle = \frac{1}{n+1}\sum_{i,j=0}^{n}(-1)^{(n-i)(n-j)}|1\rangle^i|0\rangle^{n-i} \times |0\rangle^i|1\rangle^{n-i}|1\rangle^j|0\rangle^{n-j}|0\rangle^j|1\rangle^{n-j}$$

The cost of creating this state for the teleportation trick is quite high. We must add a level of error correction to the gate [4]. Teleportation failure is equivalent to a Z measurement, so we use the following code to protect against this error:

$$\alpha|0\rangle_L + \beta|1\rangle_L \propto \alpha(|00\rangle + |11\rangle) + \beta(|01\rangle + |10\rangle)$$

Now when a physical qubit is measured in the computational basis, no quantum information is lost. This makes single-qubit operations tricky, but KLM showed that it is cheaper to use this error correction than to do teleportation with very large n [4].

We now have a near-deterministic two-qubit gate. However, if we want to do arbitrarily long quantum computations, the success probability of the gates must be close to one. Instead of making larger teleportation networks, it might be more cost effective or easier to use a form of error correction to make the gates deterministic. If we can encode against accidental measurements causing destruction of quantum information, then our qubit will be able to survive gate failures and we increase the probability of the gate eventually succeeding. KLM introduced the following logical encoding over two polarization qubits [4]:

$$\begin{aligned} |0\rangle_L &= |HH\rangle + |VV\rangle \\ |1\rangle_L &= |HV\rangle + |VH\rangle \end{aligned}$$

This is referred to as parity encoding (the logical zero state is an equal superposition of the even parity states and the logical one state is an equal superposition of the odd parity states). Consider an arbitrary qubit $\alpha|0\rangle_L + \beta|1\rangle_L$. Suppose a measurement of one of the physical qubits returns the result H. The has the following effect:

$$\alpha|0\rangle_L + \beta|1\rangle_L \to \alpha|H\rangle + \beta|V\rangle$$

That is, the qubit is not lost; we have simply reduced our encoding from parity to polarization. Similarly, if the measurement returns the result V, we have the following effect:

$$\alpha|0\rangle_L + \beta|1\rangle_L \to \alpha|V\rangle + \beta|H\rangle$$

Again the superposition is preserved, but this time a bit-flip occurs. However, the bit-flip can be corrected as it is marked by the measurement result [4].

Now suppose we wish to teleport the logical value of a parity qubit using the above teleportation operation. If we succeed we measure the value of the remaining polarization qubit and apply any necessary correction to the teleported qubit. If we fail, we can use the result of the teleportation failure to correct the remaining polarization qubit and we can then try again. In this way, the probability of success of teleportation is increased from $\frac{1}{2}$ to $\frac{3}{4}$ [4]. We have lost our encoding in the process of teleporting, but this can be fixed by introducing the following entanglement resource:

$$|H\rangle|0\rangle_L + |V\rangle|1\rangle_L$$

If the teleportation is successful, the output state remains encoded. The main observation is that the resources required to construct the entanglement resource are much less than those required to construct the teleporter. As a result, error encoding turns out to be a much more efficient way to scale up teleportation, as well as gate success correspondingly.

To boost the probability of success even further, the KLM approach uses concatenation to increase the size of the code. At the first level of concatenation the parity code states become:

$$\begin{aligned} |0\rangle_L^{(4)} &= |00\rangle_L + |11\rangle_L \\ |1\rangle_L^{(4)} &= |01\rangle_L + |10\rangle_L \end{aligned}$$

This is now a four-photon encoded state. At the second level of concatenation we would obtain an eight-photon state, etc. At each higher level of concatenation, corresponding encoded teleportation circuits can be constructed that operate with higher and higher probabilities of success [4].

If we are to use encoded qubits we must instead consider a universal set of gates on the logical encoded qubits. To achieve arbitrary single-qubit rotations we require a $\frac{\pi}{2}$ rotation about the z-axis, $Z_{\frac{\pi}{2}}$. This can be implemented on a logical qubit by applying $Z_{\pi/2}$ to each individual qubit and then applying a CZ gate between the qubits. The CZ gate is non-deterministic and so the $Z_{\frac{\pi}{2}}$ gate becomes non-deterministic for the logical qubit. We can then see that both the $Z_{\frac{\pi}{2}}$ and the logical CZ gate must be implemented with the teleportation gates in order to form a universal gate set for the logical qubits [4].

Overall the physical resources for the original KLM protocol are daunting, even though they are scalable. For linear OQC to become a viable technology, we need more efficient quantum gates.

3 Improvements on KLM

The KLM protocol explicitly tells us how to build scalable quantum computers with single-photon sources, linear optics, and photon counting. However, providing a practical architecture is a completely different matter entirely. The overhead cost of a two-qubit gate in KLM, although scalable, is unusably large. If linear OQC is to become a practical technology, we need less resource-intensive protocols. As a result, there have been a number of proposals to improve on the scalability of KLM. One such suggested area of improvement has to do with cluster-state techniques [8].

3.1 One-Way Quantum Computing with Cluster States

In the traditional approach to circuit-based quantum computing, quantum information is stored in qubits which subsequently undergo single- and two-qubit operations. However, Raussendorf and Briegle proposed an alternative model in 2001 called the cluster-state model of quantum computing [8]. This model has become an exciting alternative to existing proposals for quantum computing, and a linear optics approach is one possible implementation. With this protocol, the quantum information encoded in a set of qubits is teleported to a new set of qubits via entanglement and single-qubit measurements. This new state is called a cluster state, a collection of qubits that are entangled via nearest-neighbour CZ gates (in a rectangular lattice). Horizontal links determine the information flow, while the vertical links form the two-qubit gates. For cluster states, Yoran and Reznik realized that we do not need teleportation to succeed with a very high success probability. To support a physically feasible model, we just need a success rate of greater than $\frac{1}{2}$ [10]. Suppose the states are arranged in a lattice as shown in Figure 3. Quantum computation then consists of performing single-qubit measurements on “columns” of qubits. The outcomes of measurement on one column then determine the basis for measurement on the next column. Single-qubit gates are

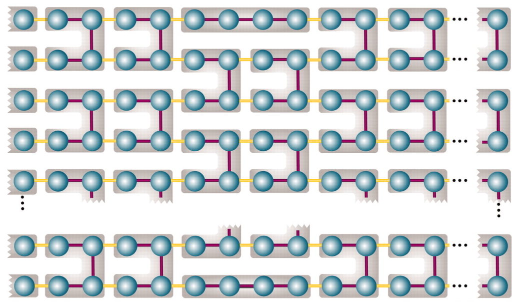

Figure 3: An example of a cluster state.

implemented by choosing a suitable basis for the next single-qubit measurement, while two-qubit gates are implemented by local measurements of two qubits with a vertical link in the cluster state. Two-dimensional cluster states (vertical and horizontal links) are essential for a complete cluster-based quantum computing model, as linear cluster-state computing can be efficiently simulated on classical computers. Since single-qubit measurements are relatively easy to perform when the qubits are photons, this approach is potentially suitable for linear OQC: given the right cluster state, we need to perform only the feed-forward post-processing and the photon detection.

4 Realistical Physical Optical Components and their Errors

In order to build a real quantum computer based on linear optics, single-photon sources, and photon detection, our design must be able to deal with errors. Although every practical implementation will have unavoidable errors, we need to ensure that these errors do not erase the quantum information that is present in the computation. The teleportation trick utilized by the KLM model employs error correction to turn the non-deterministic gates into near-deterministic gates. However, it assumes that the photon sources, the mode matching of the optical circuits, and the photon counting are all implemented perfectly. However, this is far from true in the real world.

4.1 Photon Detectors

In linear quantum optics, the main method for gaining information about the quantum states is via photon detection. There are two main types of photon detectors: ones that give the exact number of photons in the input state (number-resolving) and ones that give a binary output ("none" or "some") (bucket) [6]. The original KLM proposal relies heavily on the availability of number-resolving detectors. There are two ways a photo-detector can fail: it can either count too few photons (loss), or it can count too many photons (dark counts). The KLM architecture requires full photon-number resolving detectors with near-perfect detection efficiency and no dark counts [4]. However, the cluster state architecture can tolerate bucket detectors [8]. The detector efficiency $\eta \in [0, 1]$ can be defined operationally as the probability that a single-photon input state will result in a detector count. Dark counts can be defined as the probability that an empty (vacuum) input state will result in a detector count.

Most photon detectors in current physical implementations are bucket detectors. At this point in time, the most common detectors in experiments on linear OQC are Avalanche Photo-Diodes (APDs) [6]. When a photon hits the active semi-conductor region of an APD, it will induce the emission of an electron. The resulting current tells us that a photon was detected. As this current leads to a dead time of a few nanoseconds in the detector, any subsequent photon cannot be detected; as such, we have a bucket detector. Detectors attempting to physically realize the concept of a fully-fledged number-resolving detector are also being developed, such as the Visible Light Photon Counter (VLPC) [10]. VLPCs operate at a temperature of a few Kelvin to minimize dark counts. They consist of an active area divided into many separate active regions. A photon is detected when it triggers such a region, while all the other regions remain fully operational. However, this detecting region will still experience a dead time, meaning the VLPC may still have some detection loss.

4.2 Photon Sources

All current linear OQC protocols make critical use of perfect single-photon sources. Single-photon sources are required to not only create clean single-photon states, but all sources must also generate identical (probabilistic) states. Broadly speaking, there are currently two schemes used to realize single-photon sources: conditional spontaneous parametric down conversion (PDC), and cavity-QED Raman schemes [6]. Cavity-based single-photon sources are very complicated, and most single-photon sources used in linear OQC are instead based on PDC. However, for a practical linear OQC, we need a good microscopic single-photon source that can be produced in large numbers. A recent review on this topic by Lounis and Orrit (2005) identifies six types of microscopic sources: atoms and ions in the gaseous phase, organic molecules at low temperatures and room temperature, chromophoric systems, colour centres in diamond (such as nitrogen-vacancy or nickel-nitrogen), semiconductor nano-crystals, and self-assembled quantum dots and other hetero-structures (such as micro-pillars and micro-mesa, quantum dots, and electrically driven dots) [7].

4.3 Circuit Errors and Quantum Memories

In addition to detector errors and errors in the single-photon sources, there is a possibility that the optical circuits themselves acquire errors. The most important circuit error is likely mode mis-matching, which occurs when non-identical wave packets are used in an interferometric setup. This might occur when optical components fail to do exactly what they are supposed to do. However, most of these mode-mismatching errors are as a result of non-identical photon sources (mentioned previously). Another source of error occurs in optical components, such as beam splitters and half- and quarter-wave plates, amongst others. These are typically made of dielectric media that has a (small) absorption amplitude, resulting in occasional photon loss in the optical circuit. In large circuits, these losses can become substantial.

One final important component of linear OQC is the quantum memory. When the probability of a successful gate or addition to a cluster state becomes small, the photons that are part of the circuit must be stored for a considerable time while the off-line preparation of entangled photons is taking place. The standard use of fiber loops then becomes problematic because they induce photon losses (storing a photon for 100 μs in fiber has a loss probability of $p \approx 0.54$) [6]. At present, all linear OQC proposals need some kind of quantum memory. This may be in the form of delay lines with error correction, atomic vapours, solid-state implementations, etc. The design specifications for a solid-state based quantum memory are even more strict than those for solid-state single-photon sources as the memory not only needs to produce a single photon with very high fidelity, it also needs the ability to couple a photon into the device with very high probability.

5 General Error Correction

To achieve feasible quantum computing despite inevitable physical errors in the quantum computer, we have to employ error correction (EC). Typically, an EC protocol consists of a circuit that can correct for one or more types of errors. However, it is inevitable that these circuits will in turn introduce errors. In order for an EC protocol to be useful, the error in the circuit after the EC protocol must be smaller than the error in the circuit before the EC protocol. If this is the case, we can simply repeatedly nest the application of the EC protocol to reduce the errors to arbitrarily small levels. In doing so however, we must take care not to sacrifice the scaling behaviour of the quantum computer.

We saw that the KLM scheme employs a certain level of error correction in order to turn high-probability teleported gates into near-deterministic gates, even though the scheme assumes that all the optical components are ideal [4]. Moving past this assumption, we come to the difficult task of developing a linear OQC architecture with robustness against component errors. The three main errors that need to be coded against are inefficient detectors, noisy photon sources, and unfaithful quantum memories.

Since single-qubit measurements in linear OQC require photon detection, we have a problem: failing to measure a photon is also a single-qubit failure. Therefore, every logical qubit must be constructed with multiple photons so that we can recover from photon loss. This means that we can no longer straightforwardly remove redundant qubits in the cluster-state model if they are not properly encoded. Numerical simulations indicate that a detector loss of up to 50% can be corrected [6] (indeed, a detection efficiency of 50% is the absolute minimum [2]).

We must also keep in mind that creating large cluster states or redundant encoding in the circuit model will in turn amplify other errors, such as dephasing. Truly fault-tolerant quantum computer architectures must therefore be able to handle the actual physical noise that will be present. Given a certain noise model and EC codes, we can derive fault-tolerant thresholds: the errors must be smaller than the threshold value for concatenated error correction to eliminate them all.

6 Closing

We have now seen that it is possible to construct a quantum computer with linear optics, single-photon sources, and photon detection alone. Knill, Laflamme, and Milburn overturned the general mindset that a lack of direct photon interactions prohibits scalability [4]. However, constructing the necessary components and using fault-tolerant encoding is hard, and several groups have already proposed modifications to the KLM scheme for building a linear OQC with reduced resources and realistic (noisy) components.

The basic principles of linear OQC have all been demonstrated experimentally, predominantly using PDC and bucket photon detection. Due to the low efficiency of PDC photon sources however, these techniques cannot be considered practically scalable. As such, there is currently an effort to build the necessary single-photon sources, photon detectors, and quantum memories for a scalable linear OQC. On the theoretical side, there is an ongoing effort to design more efficient architectures and effective EC codes tailored to the noise model that is relevant to linear OQC.

Whatever the final architecture of quantum computers will be, there will always be a task for linear OQC: in order to distribute quantum information over a network of quantum computers, optical qubits will likely be the qubit of choice. Thus, the techniques reviewed here are considered by many to be an important step towards full-scale distributed quantum computing - the Quantum Internet [6].

References

[1] Andrew Childs, CS467 Lectures (2012).

[2] D. Gottesman and I.L. Chuang, *Demonstrating the Viability of Universal Quantum Computation Using Teleportation and Single-Qubit Operations*, Nature, 402 390 (1999).

[3] C.Z. Hong, Z.Y. Ou, and L. Mandel, *Measurement of sub-picosecond time intervals between two photons by interference*, Phys. Rev. Lett, 59 2044 (1987).

[4] E. Knill, R. Laflamme, and G.J. Milburn, *A scheme for efficient quantum computation with linear optics*, Nature, 409 46 (2001).

[5] E. Knill, *Quantum computing with very noisy gates*, Phys. Rev. A, 68 064303 (2003).

[6] Pieter Kok, W.J. Munro, Kae Nemoto, T.C. Ralph, Jonathon P. Dowling, and G.J. Milburn, *Linear optical quantum computing*, 1–41 (2008).

[7] B. Lounis and M. Orrit, *Single-photon sources*, Rep. Prog. Phys., 68 1129 (2005).

[8] R. Raussendorf and H.J. Briegel, *A scheme for efficient quantum computation with linear optics*, Phys. Rev. Lett., 86 5188 (2001).

[9] T.P. Spiller, W.J. Munro, S.D. Barrett, and P. Kok, *Continuous Physics*, In Press (2005).

[10] N. Yoran and B. Reznik, *Deterministic Linear Optics Quantum Computation with Single - Photon Qubits*, Phys. Rev. Lett., 91 037903 (2003).