The computational power of linear optics

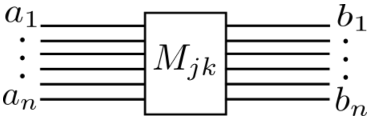
Federico Belliardo

Università di Pisa

June 11, 2019

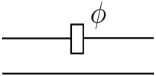
What does it means linear optics?

- Input modes $\rightarrow a_k$
- Output modes: $\rightarrow b_k$

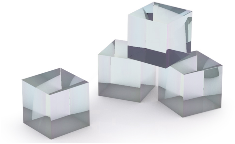


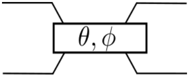
$$b_j^\dagger = \sum_k M_{jk} a_k^\dagger$$

- Waveplates, $|n\rangle \rightarrow e^{in\phi}|n\rangle$



- Beamsplitters, $\begin{pmatrix} b_1^\dagger \\ b_2^\dagger \end{pmatrix} = \begin{pmatrix} \cos\theta & -e^{i\phi}\sin\theta \\ e^{-i\phi}\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} a_1^\dagger \\ a_2^\dagger \end{pmatrix}$

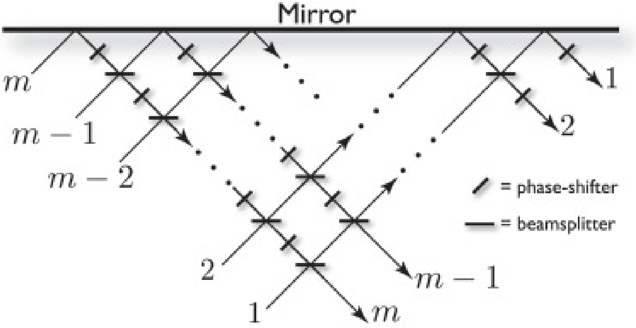




- Mirrors, Identity operators

A generic unitary U acting on the modes a_i can be decomposed in a series of beamsplitters and phase shifter.

$$U = BS_{N,N-1} \cdot BS_{N,N-2} \ldots BS_{N-1,N-3} \cdot BS_{2,1} \cdot D$$

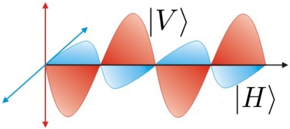


$BM_{i,j}$ is a beamsplitter applied on modes i, j and D unitary diagonal matrix representing the application of a phase shifter on each mode.

This doesn't means we have implement universal quantum computing! There is no qubit encoding in this scheme!

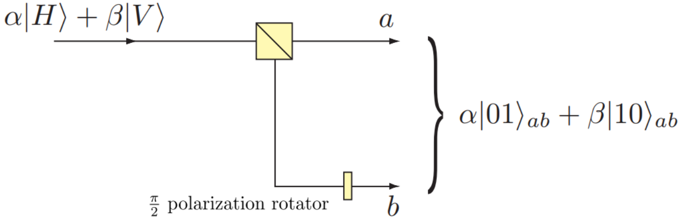
Qubit encodings

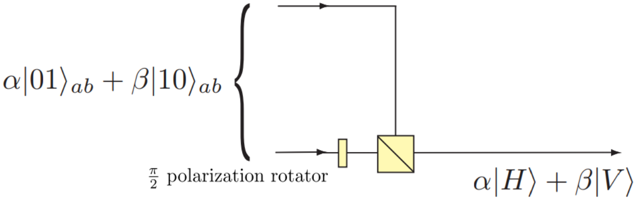
- Single rail: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (Lund & Ralph 2002). Difficult single qubit gates.
- Polarization $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$.



- Dual rail encoding $|\psi\rangle = \alpha|10\rangle + \beta|01\rangle$.

Polarization and dual rail can be converted into one another:





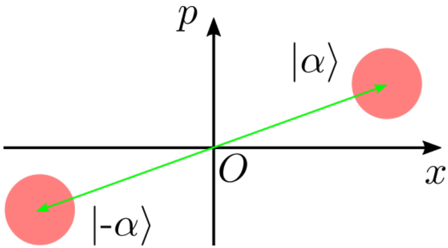
Coherent state encoding $|\psi\rangle = c_0 |\alpha\rangle + c_1 |\text{-}\alpha\rangle$.

Cons:

- Difficult single qubit gates.
- Non orthogonal $\langle\alpha|\beta\rangle \sim e^{-|\alpha-\beta|^2}$.

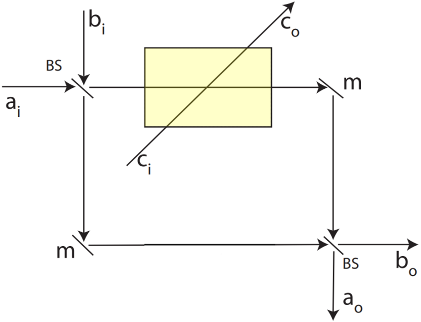
Pros:

- Easy entanglement production (beamsplitters).



How to create entanglement between photonic qubits?

Cross-Kerr non linearities $H = -\hbar\chi a_i^\dagger a_i b_i^\dagger b_i$.
If a photon is in mode c_i then $a_o = b_i$, $b_o = a_i$ (Fredkin gate, controlled SWAP).



CNOT with dual rail encoding. Strong non linearities are required.

The computational power of linear optics

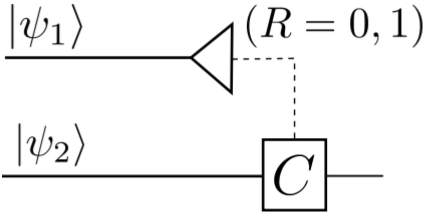
Interactions through non linear elements comes with high absorption and decoherence.

What can we do with linear optics alone?

Surprisingly linear optic allows to implement the universal quantum computer **efficiently** (with polynomial overhead).

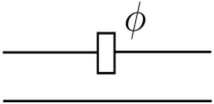
“Efficient Linear Optics Quantum Computation”
E. Knill, R. Laflamme, G. Milburn
2000

It is fundamental to have feedforward measurement: results (R) of photodetectors in midway of computation determine successive operations.

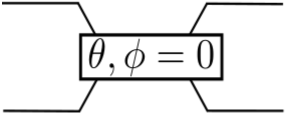


Measurement non linearity is the only required for QC!

Single qubit gates can be easily implemented with beam splitters and a phase shifter:

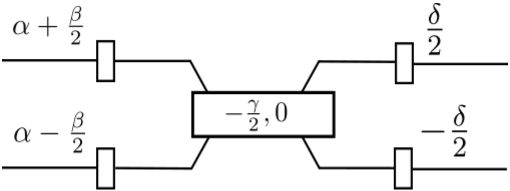


$$e^{i\frac{\phi}{2}} R_z(\phi)$$

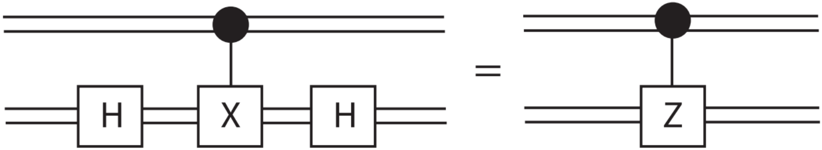


$$R_y(-2\theta)$$

Euler decomposition: $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$.



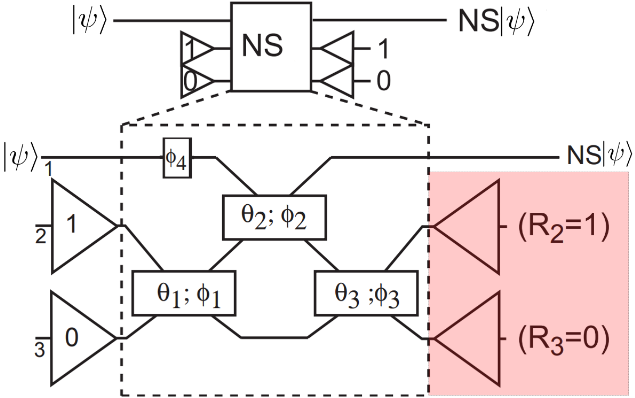
In order to do universal quantum computation we must be able to implement a CNOT (CX). Equivalently we implement a CSIGN (CZ):



We will realize CZ through an **auxiliary** NS gate.

Non linear sign shift (NS)

$$\alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle \rightarrow \alpha\,|0\rangle + \beta\,|1\rangle - \gamma\,|2\rangle$$

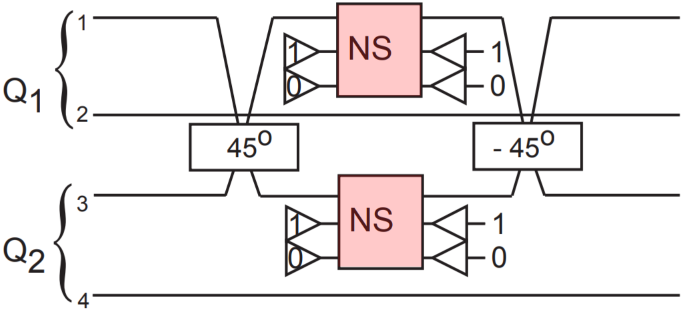


The two ancillary qubits must be measured in $R_2 = 1$ and $R_3 = 0$.

NS is a non deterministic heralded quantum gate.

The success probability of applying NS is $p = \frac{1}{4}$, but we know when it fails.

We build CSIGN via a double application of NS:



$$p = \frac{1}{4} \times \frac{1}{4} = \frac{1}{16}$$

If the gate fail the quantum information is **lost**!.
Notice that only modes 1 and 3 interact.

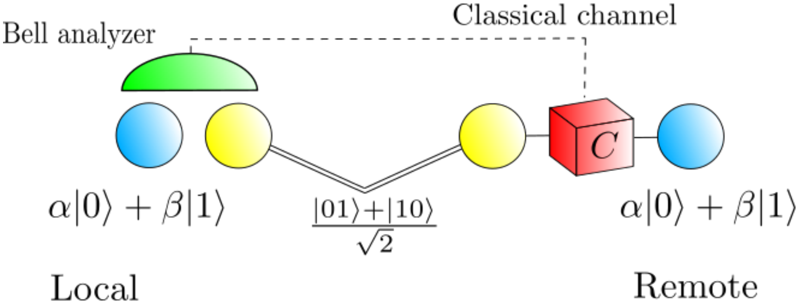
Teleportation trick

After the application of N gates the probability of success is $p^N \to 0$ ☹

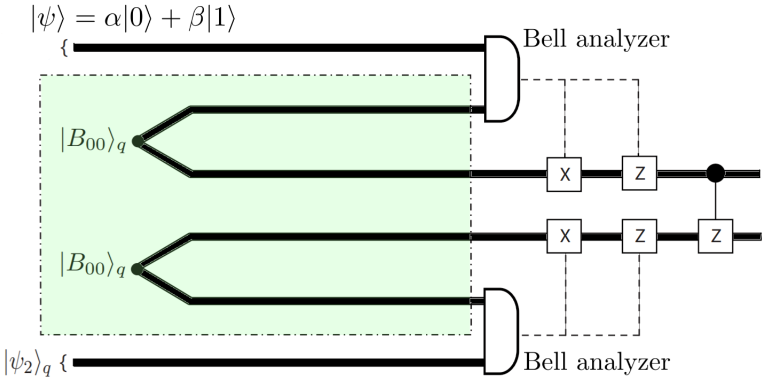
Can we make a deterministic gate? Or at least enhance the probability p of performing the computation?

Gate teleportation by Gottesman & Chuang (1999).

Qubit teleportation protocol:



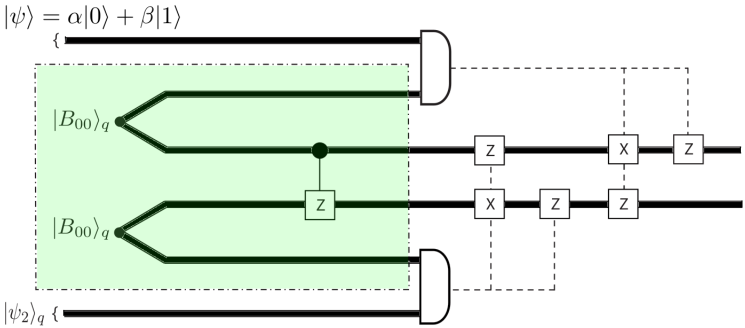
Qubit teleportation in optical modes.



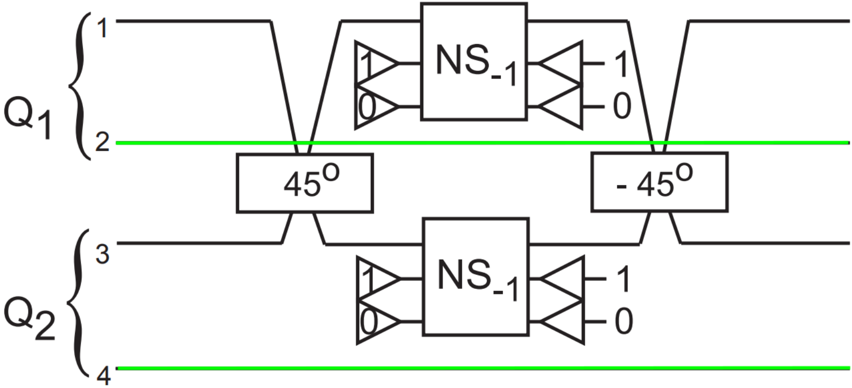
We shift the entangling gate into the preparation step (green stage) by commuting CSIGN with the classically controlled gates X and Y.

$$\begin{aligned}
\text{CSIGN}\,(\sigma_x \otimes \mathbb{1})\,\text{CSIGN} &= \sigma_x \otimes \sigma_z \\
\text{CSIGN}\,(\mathbb{1} \otimes \sigma_x)\,\text{CSIGN} &= \sigma_z \otimes \sigma_x \\
\text{CSIGN}\,(\sigma_z \otimes \mathbb{1})\,\text{CSIGN} &= \sigma_z \otimes \mathbb{1} \\
\text{CSIGN}\,(\mathbb{1} \otimes \sigma_x)\,\text{CSIGN} &= \sigma_z \otimes \sigma_x
\end{aligned}$$

CSIGN is a stabilizer of the Pauli group.



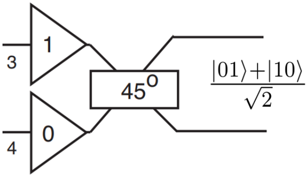
The entangling gate has gone into the preparation stage! This can be manifactured off-line probabilistically **without** spoiling the quantum information when it fails.



$$p = \frac{1}{4} \times \frac{1}{4} = \frac{1}{16}$$

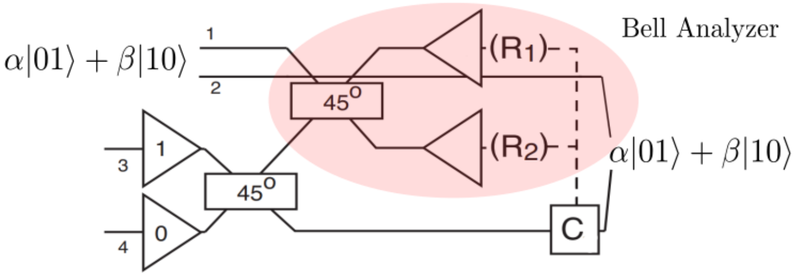
Remember that only modes 1 and 3 interact. Thus we need to teleport only two modes, not the full dual rail encoding.

The Bell state $\frac{|01\rangle+|10\rangle}{\sqrt{2}}$ can be built with a 50/50 BS:



How to perform Bell measurements with linear optics?

Teleportation of mode 1 in mode 4.



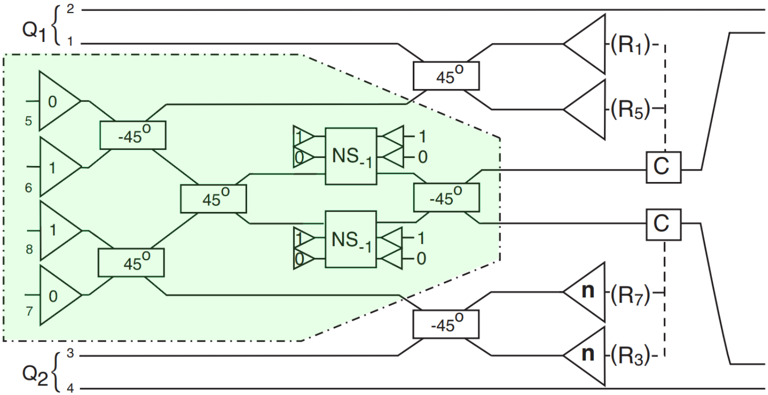
The attempted Bell measurement consist in a beamsplitter between 1 & 3 and photon counting, followed by a control C. A qubit in modes 1 & 2 gets encoded in 4 & 2.

This is **probabilistic** heralded teleportation!

$$R_1 = 0, R_2 = 1 \quad \frac{1}{2}\left(\alpha\left|01\right\rangle + \beta\left|10\right\rangle\right)$$
$$R_1 = 1, R_2 = 0 \quad \frac{1}{2}\left(-\alpha\left|01\right\rangle + \beta\left|10\right\rangle\right) \rightarrow \text{correct}$$

If a even number of photon is detected the quantum information is lost!
Success probability $p = \frac{1}{2}$.

Putting everything together:



Success probability $p = \frac{1}{4}$.

Enhanced teleportation

Deterministic Bell measurements with linear optics are impossible (Calsamiglia, 1999).

However the error probability p for teleportation can be reduced $p \to 0$ by employing a growing entangled resource to be generated offline.

Without additional resource the previous protocol $\left(p = \frac{1}{2}\right)$ is optimal.

Offline resource on $2n$ modes:

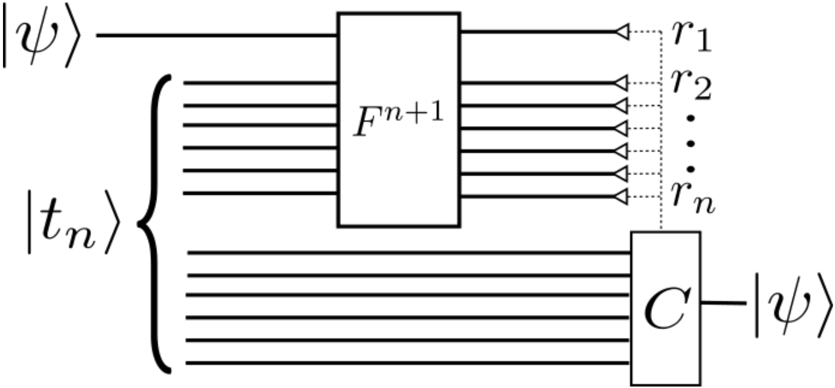
$$|t_n\rangle = \frac{1}{\sqrt{n+1}} \sum_{j=0}^{n} |1\rangle^j |0\rangle^{n-j} |0\rangle^j |1\rangle^{n-j}$$

The BS is replaced by a Quantum Fourier Transform (QFT), whose action on the modes a_j is:

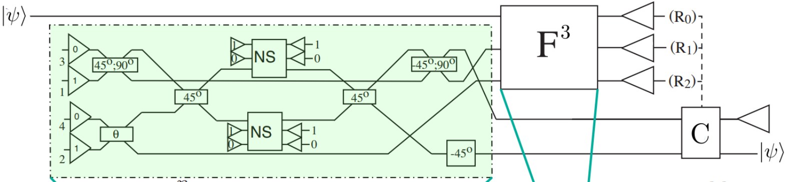
$$F_{kj}^{n+1} = \frac{e^{i\frac{2\pi kj}{n+1}}}{\sqrt{n+1}}$$

Being a unitary operator it can be decomposed in a network of BS and phase shifter with $O(n \log n)$ elements for a maximum depth of $O(\log n)$.

Count photons on the original mode and the first n modes of $|t_n\rangle$.
Each modes gives r_j photons.



Given $k = \sum r_j$ the total number of photon detected, the input qubit is teleported in mode number $n + k$. Example (for $n = 2$):



$$|t_n\rangle = \sum_{j=0}^{n} |1\rangle^j |0\rangle^{n-j} |0\rangle^j |1\rangle^{n-j}$$

$$(F_n)_{kl} = \frac{\omega^{kl}}{\sqrt{n+1}}$$

$$\omega^{kl} = e^{\frac{i2\pi}{n+1}}$$

The failure probability of teleportation is $p = \frac{1}{n+1}$.

CSIGN requires two resource states $|t_n\rangle$. The gate must be applied to every possible couple of modes, leading to:

$$
\begin{aligned}
|t_n\rangle' = \sum_j & (-1)^{(n-j)(n-i)} |1\rangle^j |0\rangle^{n-j} |0\rangle^j |1\rangle^{n-j} \\
& \otimes |1\rangle^i |n-i\rangle |0\rangle^i |1\rangle^{n-i}
\end{aligned}
$$

The failure probability for a CSIGN using $|t_n\rangle'$ is:

$$p = 1 - \left(\frac{n}{n+1}\right)^2 < p_{thr}$$

Choose n large enough that the failure probability is lower than the **threshold** for fault tolerant quantum computation.

This proves linear optics can implement **efficiently** (with polynomial overhead) a quantum computer!

KLM showed that the required number of elementary operations needed to implement the offline resource $|t_n\rangle$ is $2^{O\left(\sqrt{n}\right)}$.

n is a constant it doesn't affect the resource requirement in the scaling of the quantum computer.

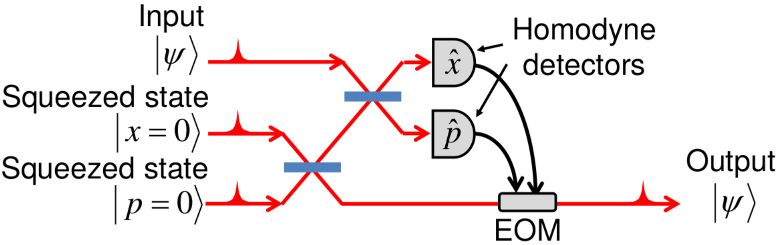
For a failure probability of $p = 0.5\%$, $n = 400$ is required, with at least 10^6 elementary operations.

The resources for a single gate can become astronomic!

This is a proof of concept, more feasible approach to perform quantum computing with optics are needed.

Teleportation

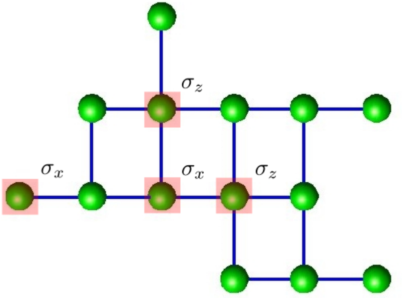
The teleportation of a gaussian state is deterministic.



The squeezing ratio limits the fidelity. An hybrid qubit could be:

$$|\psi\rangle = c_0 |01\rangle |\alpha\rangle + c_1 |10\rangle |-\alpha\rangle$$

All the computational effort is transferred offline by producing an entangled cluster state universal for computation.



The computation is done through single qubit measurements on the cluster.

Photonic architecture

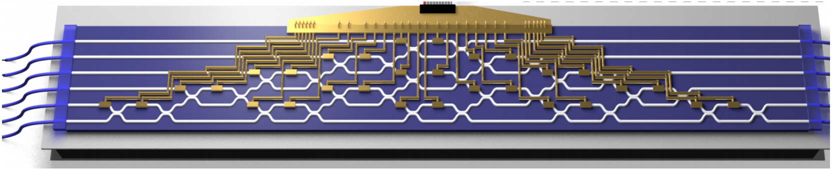
Pros:

- Photons makes excellent flying qubits.
- Negligible stochastic noise.
- Does not require mK temperatures (actually efficient detectors are superconductive).
- No atomic-scale fabrication.

Cons:

- Photon loss (erasure channel).
- Difficult to create entanglement.

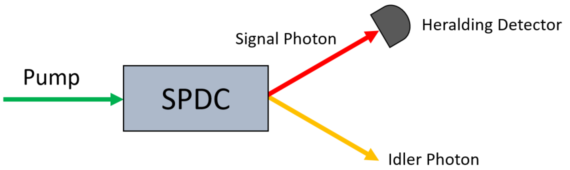
Photonic technology can be integrated using silica waveguides on a silicon chip.



Picture taken from "Universal Linear Optics" (Carolan, 2015).

Technological problems

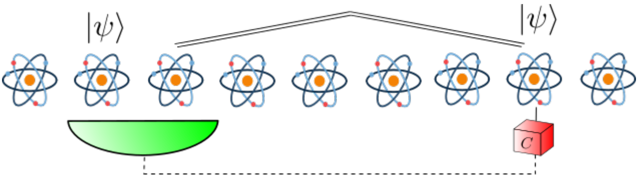
- Reliable source of single photons (above the threshold for EC)
- Reliable detector (superconductors)
- Synchronization of sources.
  SPDC emits an entangled pair at random time, it is heralded but how to synchronize photon emission from different sources?



Generation of a clock?

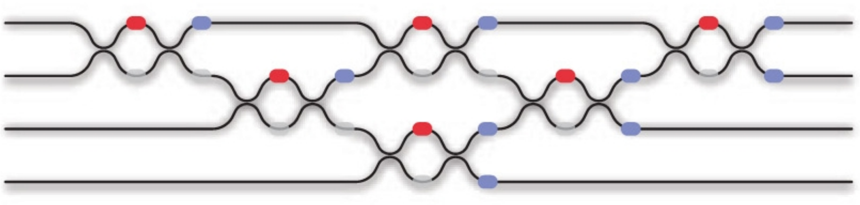
To apply the threshold theorem all the gates must be below the same level of noise. Also if they entangle qubit 1 with qubit $N \gg 1$.

Entanglement between non-adjacent qubits can be done by a series of SWAP (error accumulates) or via teleportation with offline distilled entanglement.

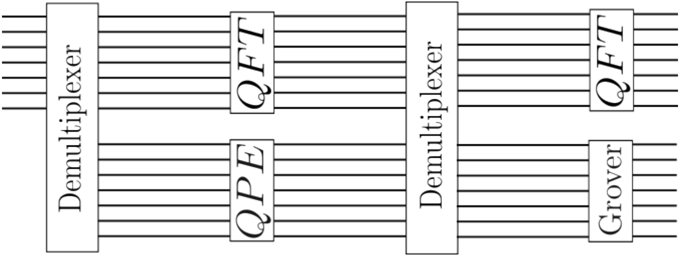


Connectivity problem - Qubit Bus!

In a photonic architecture the relevant qubits can simply come closer travelling in the integrated waveguide.



Integrated photonic circuits will have limited programmability (with respect to current platform).
They might come in printed modules: QFT, QPE, Grover, ...
High level quantum programming will consist in putting together modules via demultiplexing:

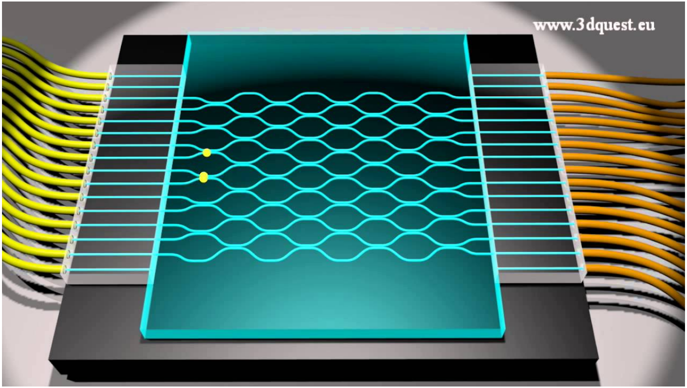


"There are a million ways to make one qubit...
...But only one way to make a million qubits"

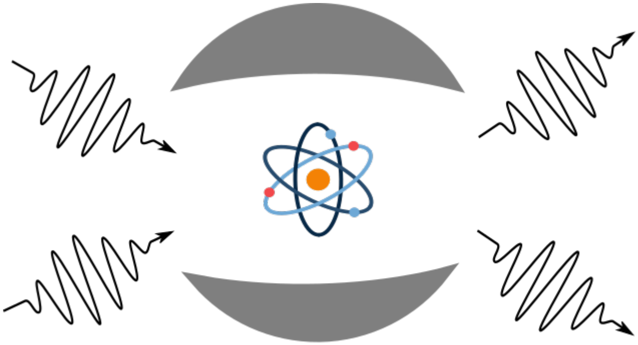
(Terry Rudolph)

Thanks!

What if we don't have feedforward measurements?



The model is called BosonSampling and is still hard to simulate classically (Aaronson, Arkhipov 2013).



Cs

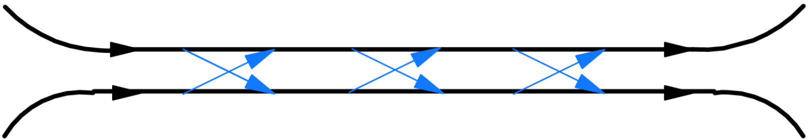
Non linear effects in QED cavities (Turchette, 1995).

Right or left circular polarization codify the qubit:

$$
\begin{aligned}
|1^-1^-\rangle &\rightarrow |1^-1^-\rangle \\
|1^+1^-\rangle &\rightarrow e^{i\phi_a}\,|1^+1^-\rangle \\
|1^-1^+\rangle &\rightarrow e^{i\phi_b}\,|1^+1^-\rangle \\
|1^+1^+\rangle &\rightarrow e^{i(\phi_a+\phi_b+\Delta)}\,|1^+1^+\rangle
\end{aligned}
$$

$$
\begin{aligned}
\phi_a &= (17.5 \pm 1)^\circ \\
\phi_b &= (12.5 \pm 1)^\circ \\
\Delta &= (16 \pm 3)^\circ
\end{aligned}
$$

Mixing two modes in a **two** photon absorption material, with low single photon absorption and low loss.



Effectively suppress HOM via Zeno effect and performs $\sqrt{SWAP}$ (Franson, 2004).