Rohit Ramakrishnan
Applied Photonics Lab, ECE

Quantum Information Technology

ECE Student Seminar Series

Indian Institute of Science Bangalore

Overview

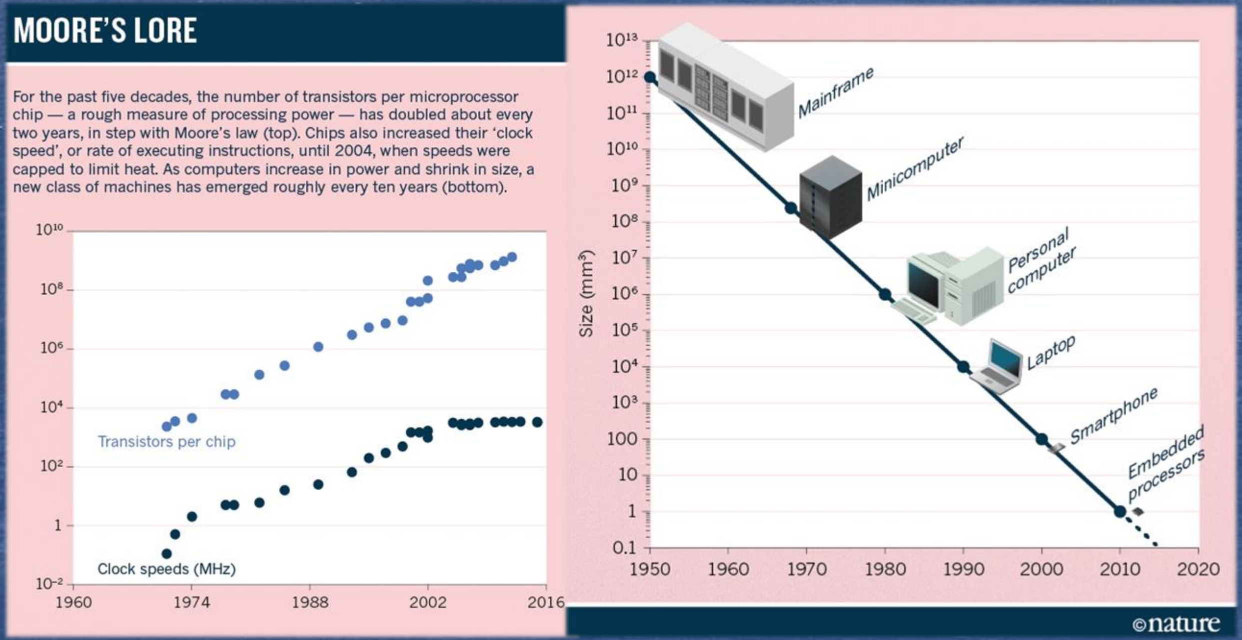
- Quantum Computers
  - Quantum bits
  - Quantum gates
  - Bell States
  - Entanglement
- Quantum Communication
  - Quantum Teleportation
  - QKD
  - HD QKD
  - Recent developments

What is a Quantum Computer?

A Quantum computer is a computing device which harnesses quantum mechanical phenomena to process information

Why do we need a Quantum Computer?

- **“Moore’s Law Is Dead. Now What?”,** MIT Technology Review, May 13, 2016
- **“The chips are down for Moore’s law”** Nature 530, February 11, 2016



History

Richard Feynman (1981):

"...trying to find a computer simulation of physics, seems to me to be an excellent program to follow out...and I'm not happy with all the analyses that go with just the classical theory, because *nature isn't classical*, dammit, and if you want to make a simulation of nature, you'd better *make it quantum mechanical*, and by golly it's a wonderful problem because it doesn't look so easy."

History

- 1981 – Feynman proposes the idea of Quantum computation
- 1985 – David Deutsch develops the Quantum Computing Model
- 1994 – Peter Shor comes up with a quantum algorithm to factor very large numbers in polynomial time
- 1997 – Lov Grover develops a quantum search algorithm

The Quantum Bit - Qubit

The quantum "version" of classical bit

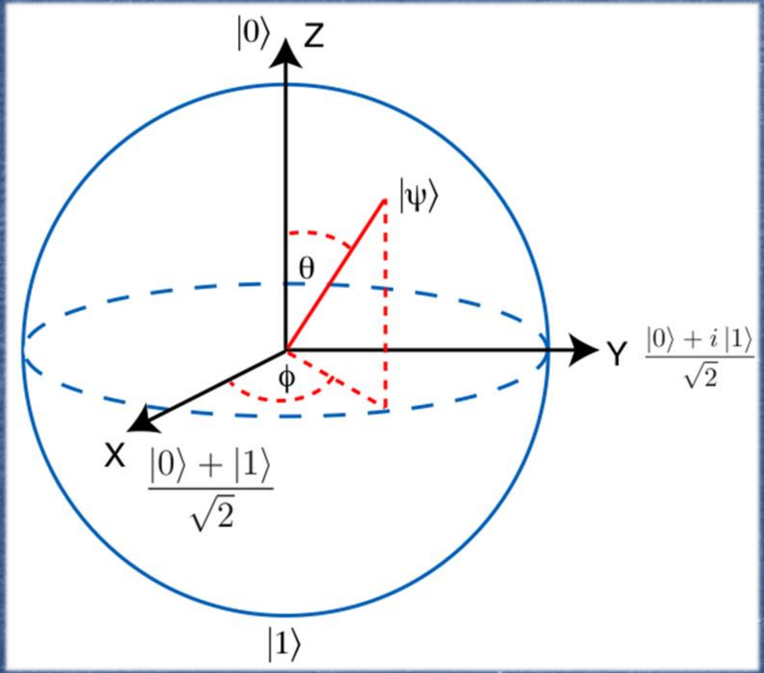
$0 \longrightarrow |0\rangle$ $\qquad 1 \longrightarrow |1\rangle$

Quantum Superposition $\quad |\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Probability of getting 0 is $|\alpha|^2$

Probability of getting 1 is $|\beta|^2$ $\qquad |\alpha|^2 + |\beta|^2 = 1$

The Quantum Bit - Qubit



Bloch Sphere

Image courtesy: IBM

$$|\Psi\rangle = e^{i\gamma}\{\cos\frac{\theta}{2}|0\rangle + e^{i\varphi} sin\frac{\theta}{2}|1\rangle\}$$

where γ, θ, φ are real numbers

Multiple Qubits

$00 \longrightarrow |00\rangle$

$01 \longrightarrow |01\rangle$

$10 \longrightarrow |10\rangle$

$11 \longrightarrow |11\rangle$

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

Quantum Gates (Single Qubit gates)

Pauli gates

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Hadamard gate

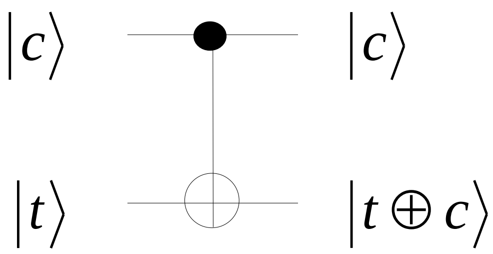
$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}; \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}; \quad H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Multi Qubit Gates

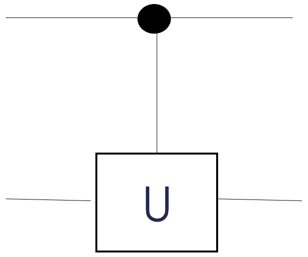
C NOT Gate

Control

Target



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



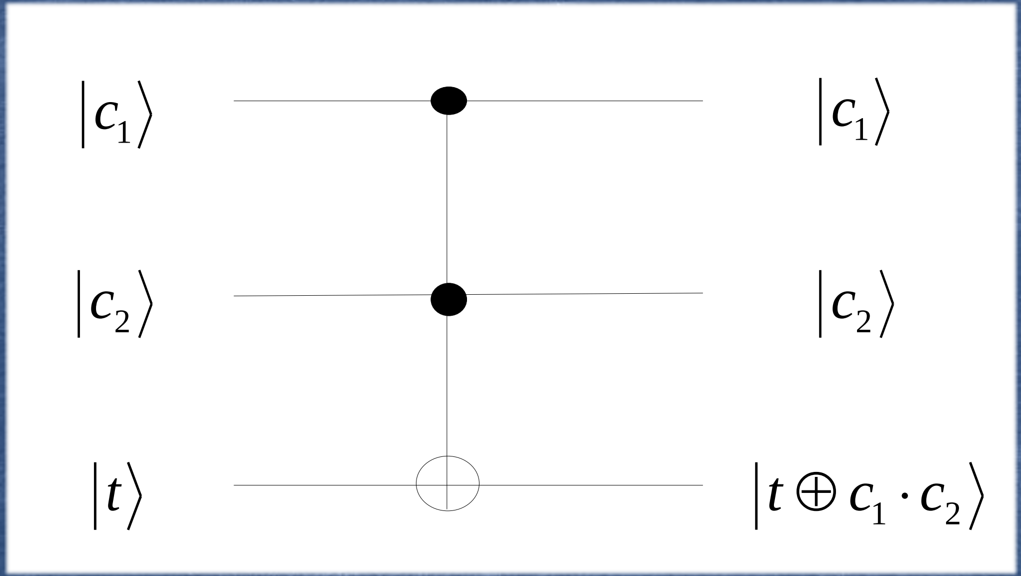
Multi Qubit Gates

Toffoli gate [CCNOT Gate]

Control qubit 1

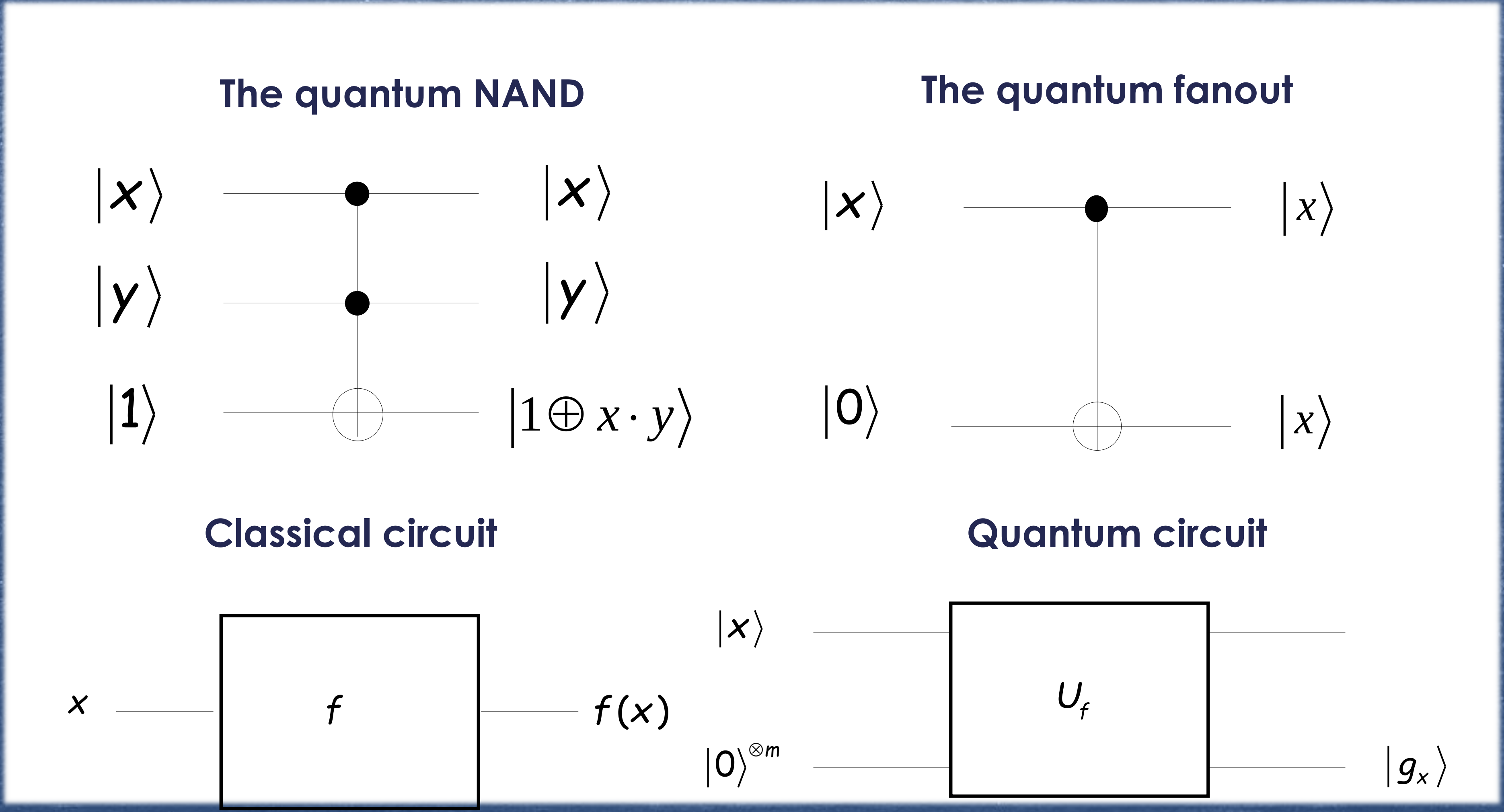
Control qubit 2

Target qubit



$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

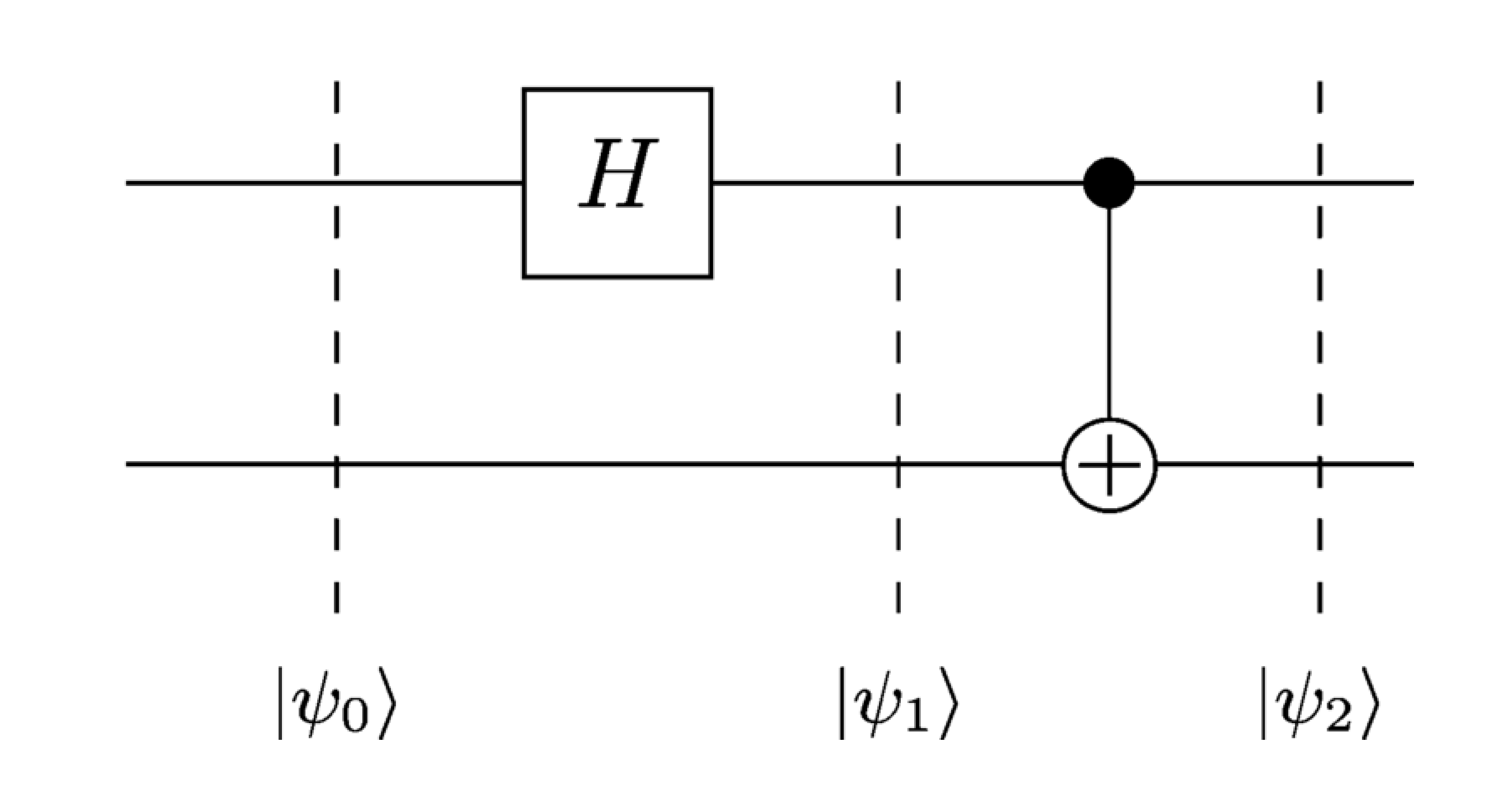
Quantum Analogues of Classical gates



DiVincenzo Criteria

- A scalable physical system with well characterized qubits.
- The ability to initialize the state of the qubits to a simple fiducial state.
- Long relevant decoherence times.
- A "universal" set of quantum gates.
- A qubit-specific measurement capability.
- The ability to interconvert stationary and flying qubits.
- The ability to faithfully transmit flying qubits between specified locations.

Bell Measurement



Quantum Entanglement

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

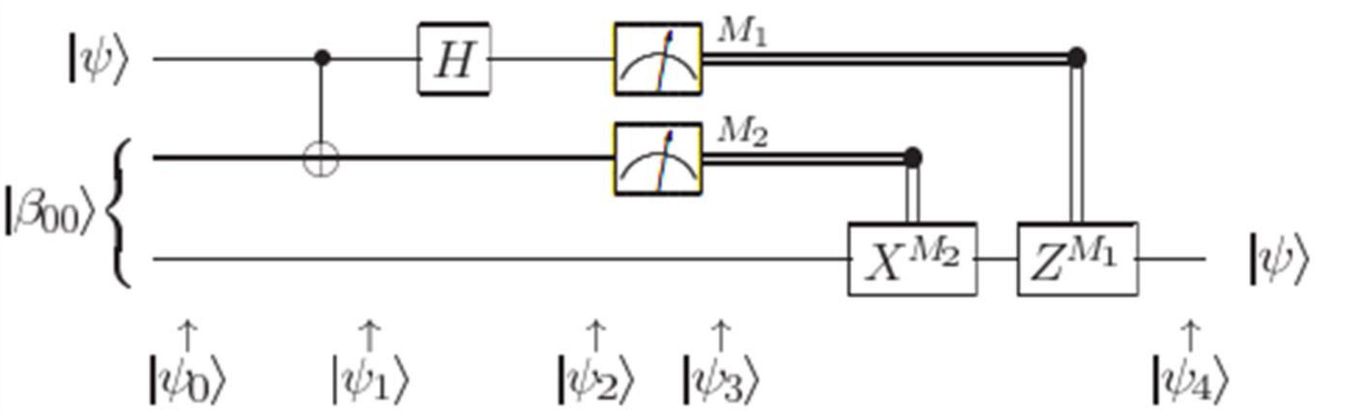
$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

- Non local correlations exhibited by a set of qubits
- They cannot be expressed as product of 2 states

Quantum Teleportation



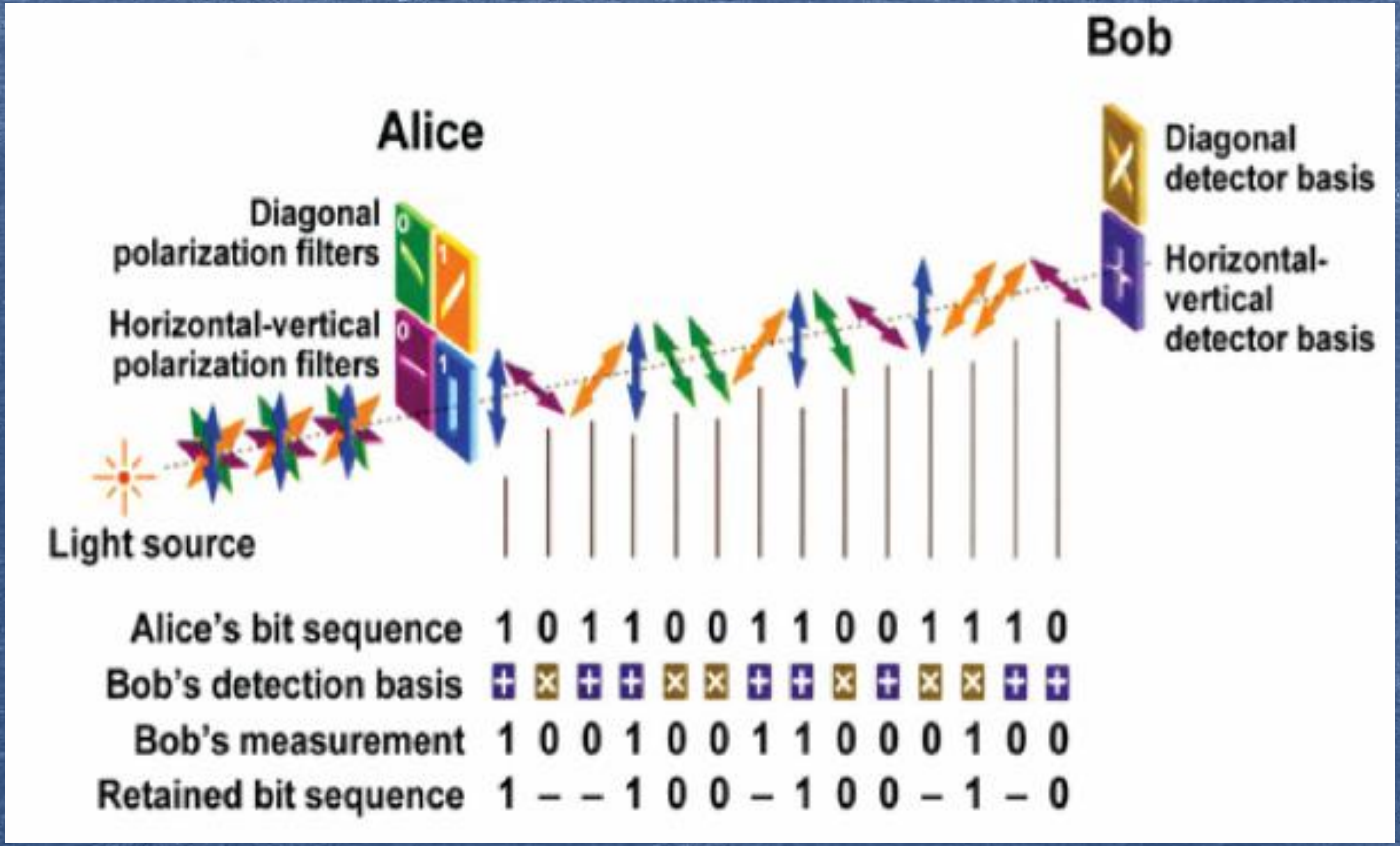
Quantum circuit for teleporting a qubit. The two top lines represent Alice's system, while the bottom line is Bob's system. The meters represent measurement, and the double lines coming out of them carry classical bits (recall that single lines denote qubits).

Ref: Nielsen and Chuang "Quantum Computation and Quantum Information"

Quantum Cryptography

- BB 84 Protocol
- E91 Protocol

BB84 Protocol



High Dimensional Quantum Cryptography

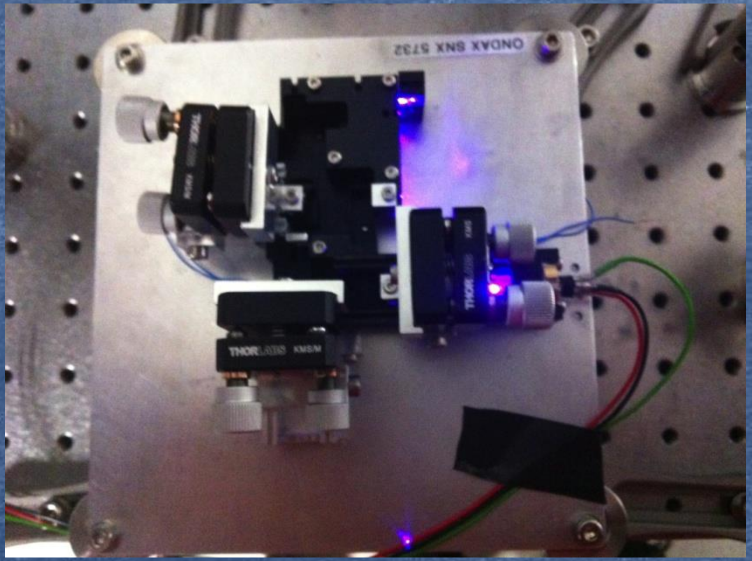
- Encode more information per quantum state

- Use “Qudits” instead of “Qubits”
  - Generalization of Qubit in to d-state systems

When can we have them?

- Quantum Computers
  - D Wave (2011, 2012, 2015)
  - IBM (2016, 2017)
  - Intel (2017)
  - Google (2019)
  - Volkswagen (tied up with Google)
  - Alibaba (2017)
  - NASA (2012)

When can we have them?



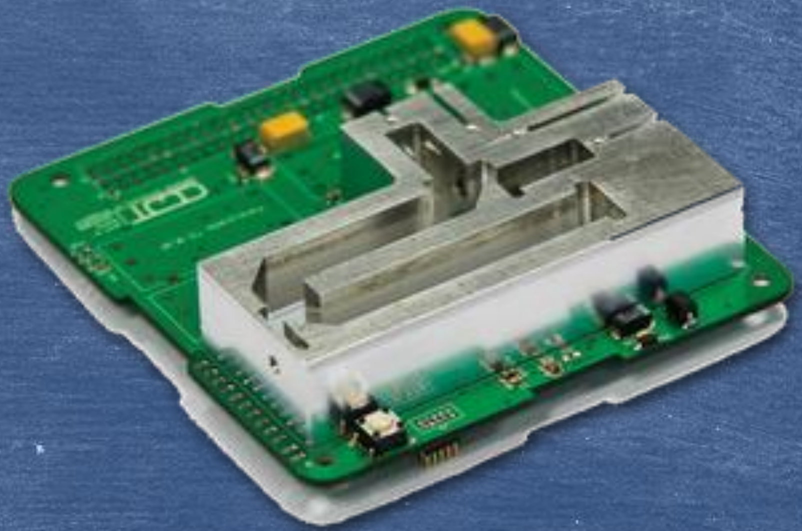


Image Courtesy: Center for Quantum Technologies, NUS, Singapore

When can we have them?

- Quantum Communications

  Chinese Satellite Micius

  (August 2016 by Jian Wei Pan's group)

- Quantum Internet (2020)

Questions

THANK YOU !