

Quantum Computation: Technology for the Day After Tomorrow

by

Bob Pedigo

rmpedigo@ieee.org

IEEE Hampton Roads Section

March 17, 2005





Happy St. Patrick's Day!



Overview

Quantum Mechanics Primer

Einstein's Challenge

What, Why, & How?

Continuing Obstacles

Current State of Practice

Future of Quantum Computation

Background Needed

Linear Algebra

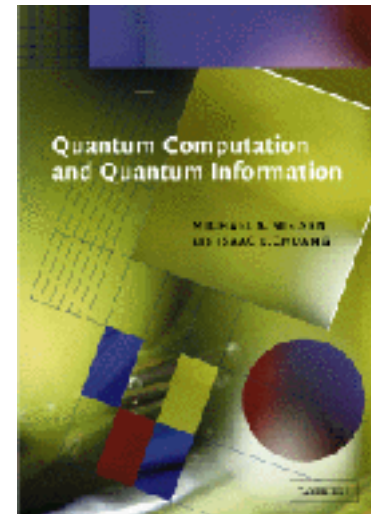
Hilbert Spaces

Quantum Mechanics

Information Theory

Algorithm Design

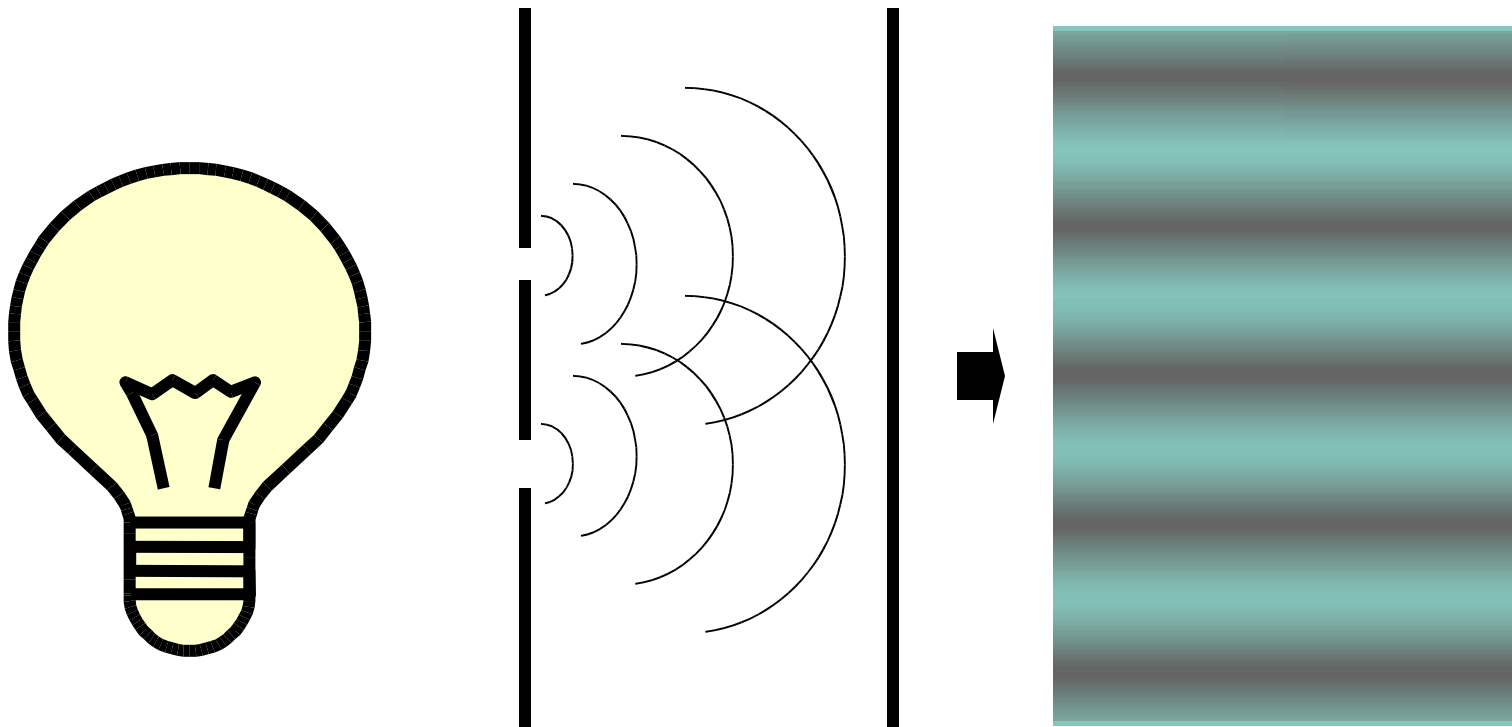
Computer Logic/Circuit Design



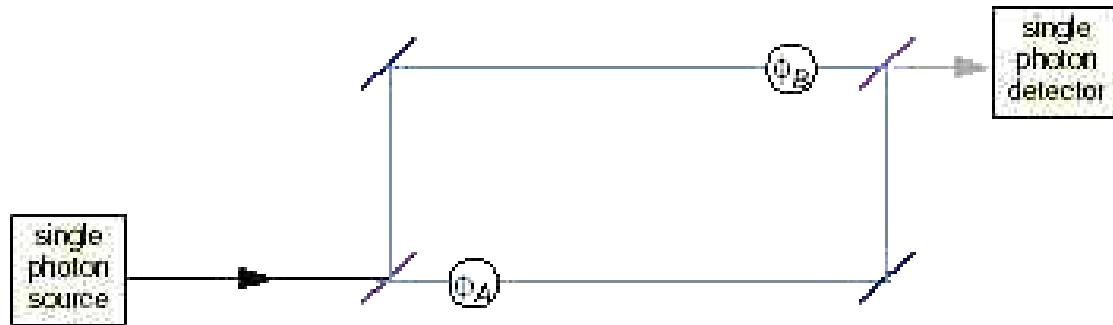
The “strangeness” of quantum mechanics

A quick lesson...

Classical “Double Slit” Experiment



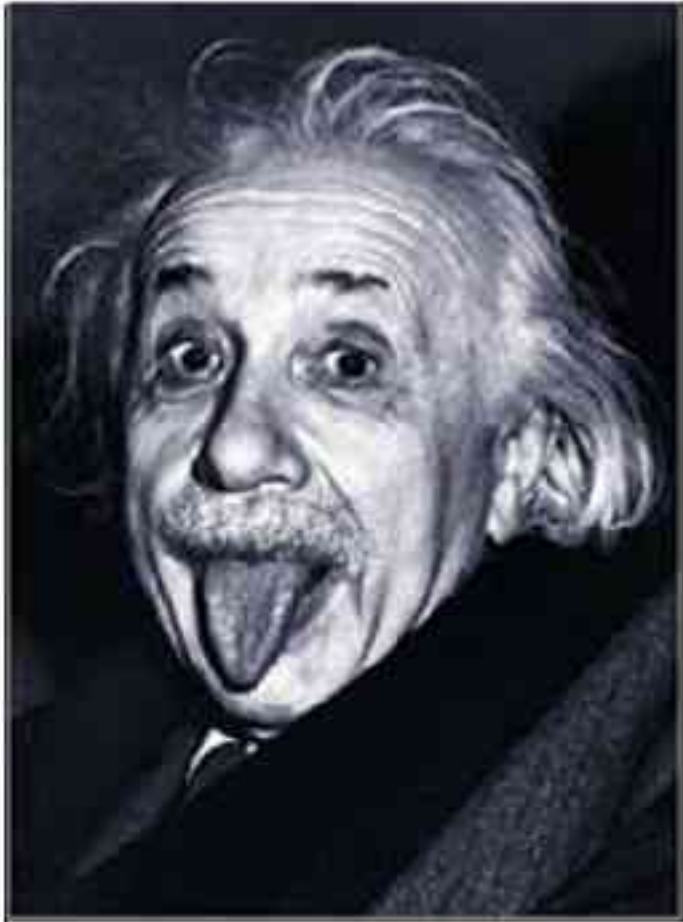
Simple Light Interference Experiment (“updated double-slit”)



Reference: Hughes, et.al., “Quantum Cryptography.” Los Alamos National Lab. 1995.

Einstein's Challenge (1935)

“God doesn't play dice with the world.”



**EPR paper in 1935
pointed out
fundamental
conflicts with
quantum
mechanical theory:
“spooky action at
a distance”**

Bell's Solution (1964)

Bell finally resolves discrepancy and saves quantum mechanics

Solution: information flow is “...part of the system...”

Without this solution, quantum computing would not have been born!

What is Quantum Computation?

Computing via quantum mechanics rather than electrical circuits

Heisenberg's Uncertainty Principle

Superposition of states

Entanglement

**No more moving bits through wire;
QC moves logic operations through
time across stationary memory
register of “qubits”**

Why is Quantum Computing Necessary?

We have reached the physical limits of microchip design

Moore's Law in jeopardy

Quantum mechanical properties can no longer be ignored

We still haven't solved the *really* tough problems of math & science

What Quantum Computation can Provide Us

Moore's Law can be preserved

RSA can be broken!

Totally secure communications

Fast, robust database searches

Simulate complex biological & quantum systems

How Does QC Do All This?

Classical Computing: Bit = 0 or 1

**Quantum Computing: Qubit = 0, 1, or
*Both***

**...which leads to *simultaneous*
*calculations***

Quantum Logic

“Any multiple qubit logic gate may be composed from CNOT and single qubit gates.” -- Nielson & Chuang, pg. 22

Quantum algorithms are *reversible*

“No-Cloning theorem” disallows copying of unknown quantum states

Continuing Difficulties

Heisenberg's Uncertainty Principle

Makes QC possible

Makes it hard to measure

Decoherence

Can be mitigated with error-correcting codes

Causes lots of overhead; reduces efficiency

Cost/Practicality of current protocols

Distance Limits

Who's Working on QC today?

Academia:

Univ. of Wisconsin, Madison

Univ. of York, UK

CalTech

Oxford Univ., UK

Stanford/Berkeley/MIT

Who's Working on QC? (2)

Private Sector:

IBM



Bell Labs

MagiQ Technologies



Microsoft



Who's Working on QC? (3)

Public Sector:



Who's Working on QC? (4)

Other nations:

Japan

China

India

France

Germany

Russia

Switzerland

Australia

*And the list goes
on...*

Current State of the Practice

Teleportation demonstrated in lab

Bit registers up to 10 qubits

Algorithms for fast searching of unstructured databases

Solid state qubits demonstrated in lab

Current State of the Practice



Product: Quantum Cryptography

Vendor: **MagiQ Technologies**

Est. Cost: **Estimated \$50,000**

Product Website: <http://www.magiqtech.com/>

Commercial encryption devices now available

What's Next?

Improving free-space & fiber quantum transmission channels

Implementing QKD using solid state technologies

Increasing qubit memory registers to improve performance and capacity

Making QKD affordable

What The Future Holds

**Totally secure communications
anywhere, anytime**

Faster information processing

**Solve “computationally difficult”
problems**

Quantum Resources

Feynman Lectures on Computation, Hey and Allen (eds.), Perseus Publishing, 1996.

The Physics of Quantum Information, Bouwmeester, et. al. (eds.), Springer, 2000.

Quantum Computation and Quantum Information, Nielsen and Chuang, Cambridge Univ. Press, 2000.

“*E-print Archive*”: <http://xxx.lanl.gov>

Quantum Computation

Questions?

Quantum Computation

Backups

What is Quantum Teleportation?

Is it Star Trek?

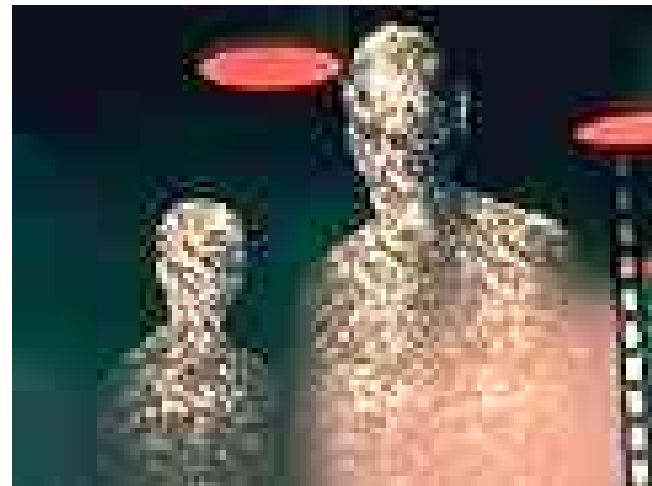
No!

Is it magic?

No!

**Will it enable
instantaneous
travel?**

No!



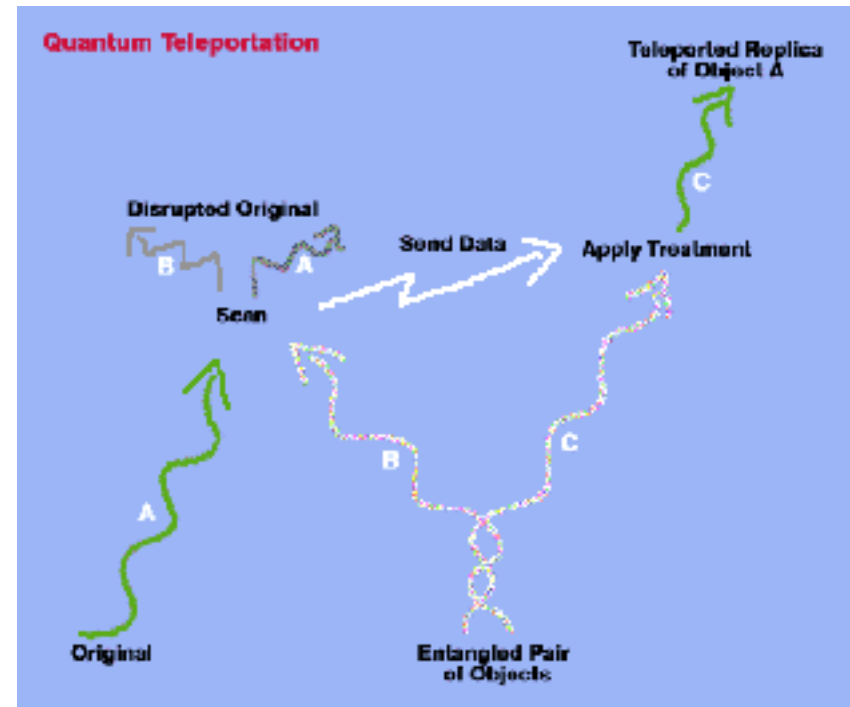
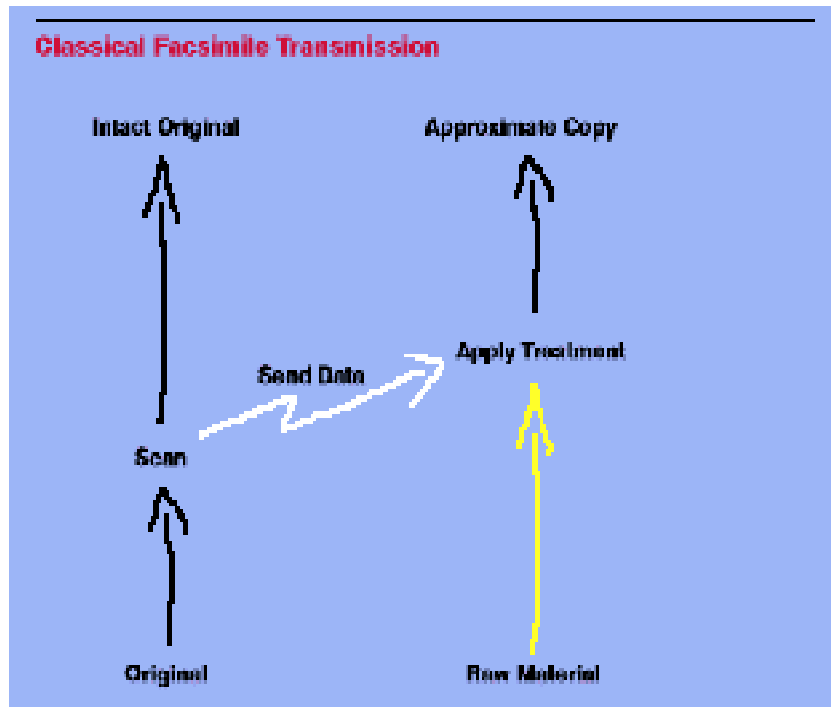
What is Quantum Teleportation?

Transfer of information without physical transportation

Unique to quantum mechanical world

Key: destroys original, leaving “new original” in teleported location

What is quantum teleportation?



**Diagrams courtesy of IBM Research, Inc., 1995.*