Quantum Computing

Sushain Cherivirala

Quantum Computing

Bits and Qubits

Quantum Gates

Measurement of Qubits

More Quantum Gates

Universal Computation

Entangled States

Superdense Coding

Measurement Revisited

Quantum Teleportation

Surprise?

Quantum Computing

Bits and Qubits

Quantum Gates

Measurement of Qubits

More Quantum Gates

Universal Computation

Entangled States

Superdense Coding

Measurement Revisited

Quantum Teleportation

Surprise?

Bits and Qubits

The fundamental units of information

Bits and Qubits

Classical Bits (light switch)

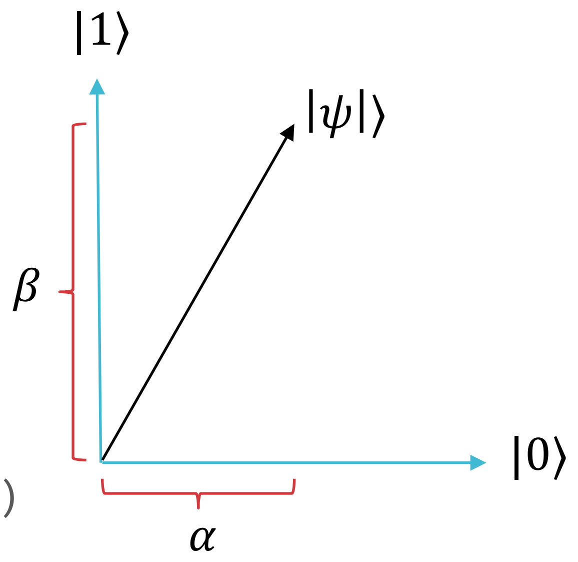
0 and 1

Quantum Bits

Computational Basis States

$|0\rangle$ and $|1\rangle$ (Dirac/bra-ket notation)

$\begin{bmatrix}1\\0\end{bmatrix}$ and $\begin{bmatrix}0\\1\end{bmatrix}$ (vector in complex space notation)



General Quantum State

$\alpha|0\rangle + \beta|1\rangle = \begin{bmatrix}\alpha\\\beta\end{bmatrix} = |\psi|\rangle$ with α and β as amplitudes

$|\alpha|^2 + |\beta|^2 = 1$ (normalization condition – unit vector)

Start with mathematical description then develop physical intuition for results

Quantum Computing

Bits and Qubits

Quantum Gates

Measurement of Qubits

More Quantum Gates

Universal Computation

Entangled States

Superdense Coding

Measurement Revisited

Quantum Teleportation

Surprise?

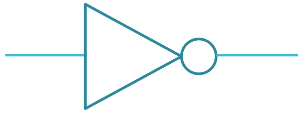
Quantum Gates

Manipulation of bits (computation) builds logical systems (computers)

NOT Gate

Classical NOT gate

$$\begin{cases} 0 \rightarrow 1 \\ 1 \rightarrow 0 \end{cases}$$

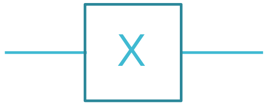


Quantum NOT gate (Pauli-X gate)

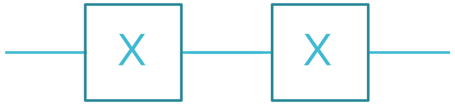
$$\begin{cases} |0\rangle \rightarrow |1\rangle \\ |1\rangle \rightarrow |0\rangle \end{cases}$$

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|1\rangle + \beta|0\rangle$$

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{(Pauli matrix)}$$



$$XX = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \text{ (Identity matrix)}$$

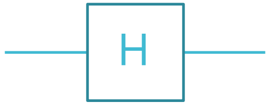


Quantum NOT gate and Classical NOT gate are practically equivalent

Hadamard Gate

Hadamard Gate

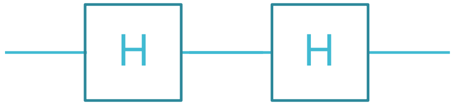
$$\begin{cases} |0\rangle \rightarrow \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ |1\rangle \rightarrow \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{cases}$$



$$\alpha|0\rangle + \beta|1\rangle \rightarrow \frac{\alpha+\beta}{\sqrt{2}}\,|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$$

$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$ (Hadamard matrix)

$$HH = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = I$$



$H' = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}$, $\|H'|0\rangle\| \neq 1$ (not normalized)

Useful in taking shortcuts, similar to quantum tunneling, by expanding the states computer can assume

Quantum Computing

Bits and Qubits

Quantum Gates

Measurement of Qubits

More Quantum Gates

Universal Computation

Entangled States

Superdense Coding

Measurement Revisited

Quantum Teleportation

Surprise?

Measurement of Qubits

Computation is pointless without measurement of results

Measurement in the computation basis

Quantum state **not directly observable** from a qubit

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \begin{cases} 0\ with\ P = |\alpha|^2 \\ 1\ with\ P = |\beta|^2 \end{cases}$$

Measurement **disturbs** state, results in a computational basis state

$|\alpha|^2 + |\beta|^2 = 1$ (normalization constraint)

HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
Dilbert.com DilbertCartoonist@gmail.com
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
4-17-12 © 2012 Scott Adams, Inc./Dist. by Universal Uclick
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.

Quantum Computing

Bits and Qubits

Quantum Gates

Measurement of Qubits

More Quantum Gates

Universal Computation

Entangled States

Superdense Coding

Measurement Revisited

Quantum Teleportation

Surprise?

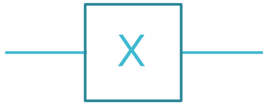
More Quantum Gates

Gates, unitary transformations, serve as primitives for computation

General single-qubit Gates

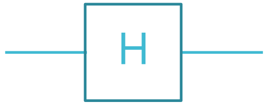
Pauli-X (NOT) Gate

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



Hadamard Gate

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$



General Single-qubit Gate

$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ (Unitary matrix)

$U^{\dagger}U = I$ where $U^{\dagger} = (U^{T})^{*}$

Preservation of length

$$\| U|\psi\rangle \| = \| |\psi\rangle \|$$

Preservation of length is the unique property of unitary matrices

Phase shift Gates

$$\begin{cases} |0\rangle \rightarrow e^{i\theta}|0\rangle \\ |1\rangle \rightarrow e^{i\phi}|1\rangle \end{cases}$$

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha e^{i\theta}|0\rangle + \beta e^{i\phi}|1\rangle$$

$$R_{\theta,\phi} = \begin{bmatrix} e^{i\theta} & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

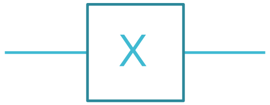
At first glance, $\alpha e^{i\theta}|0\rangle + \beta e^{i\phi}|1\rangle$ is not distinguishable from $\alpha|0\rangle + \beta|1\rangle$ but can be made so through the Hadamard gate

$$R_{\theta} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

Pauli Gates

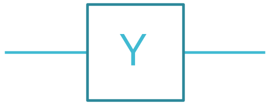
Pauli X-Gate

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



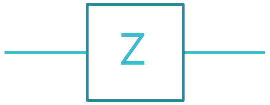
Pauli Y-Gate

$$Y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}$$



Pauli Z-Gate

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



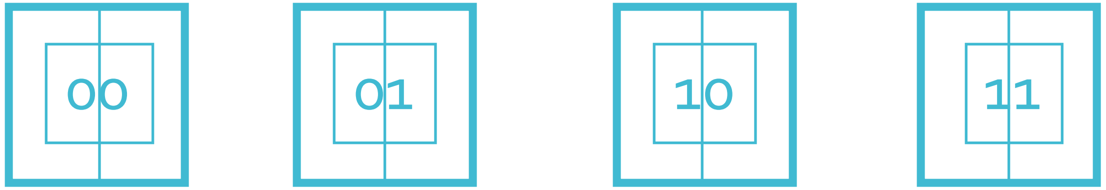
Controlled-NOT Gate (C-NOT)

Final gate that is essential, all else can be built upon it

Computational basis: $\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = \begin{bmatrix}\alpha \\ \beta \\ \gamma \\ \delta\end{bmatrix}$

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

$$\begin{cases} |00\rangle \rightarrow |00\rangle \\ |01\rangle \rightarrow |01\rangle \\ |10\rangle \rightarrow |11\rangle \\ |11\rangle \rightarrow |10\rangle \end{cases}$$



00

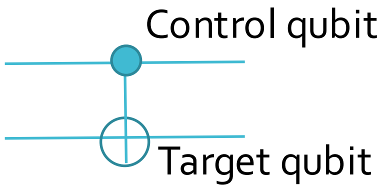
01

10

11

$$|xy\rangle \rightarrow |x(y \oplus x)\rangle \qquad |xyz\rangle \rightarrow |xy(z \oplus y)\rangle$$

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



Quantum Computing

Bits and Qubits

Quantum Gates

Measurement of Qubits

More Quantum Gates

Universal Computation

Entangled States

Superdense Coding

Measurement Revisited

Quantum Teleportation

Surprise?

Universal Computation

Only a small set of primitives is necessary for building complex systems of grand proportions

Classical Universality

Universal single gates are the NOR and NAND gates.

NOR gate = NOT gate + OR gate

NAND gate = NOT gate + AND gate

Universal set of gates sufficient for all classical computation

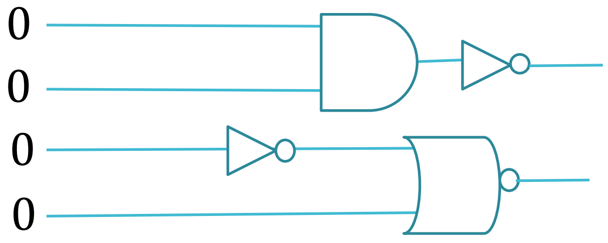
Quantum Universality

CNOT and single-qubit gates provide quantum universality for any unitary quantum operation on n qubits

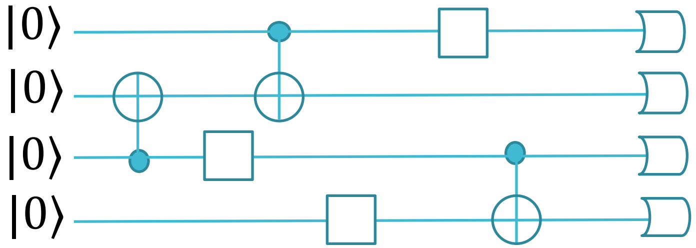
Circuit Models

Can be shown that all classical systems can be converted into equivalent quantum systems of roughly the same size

Numerous equivalent models exist that describe quantum systems, quantum circuit model has an analogy in Classical computing



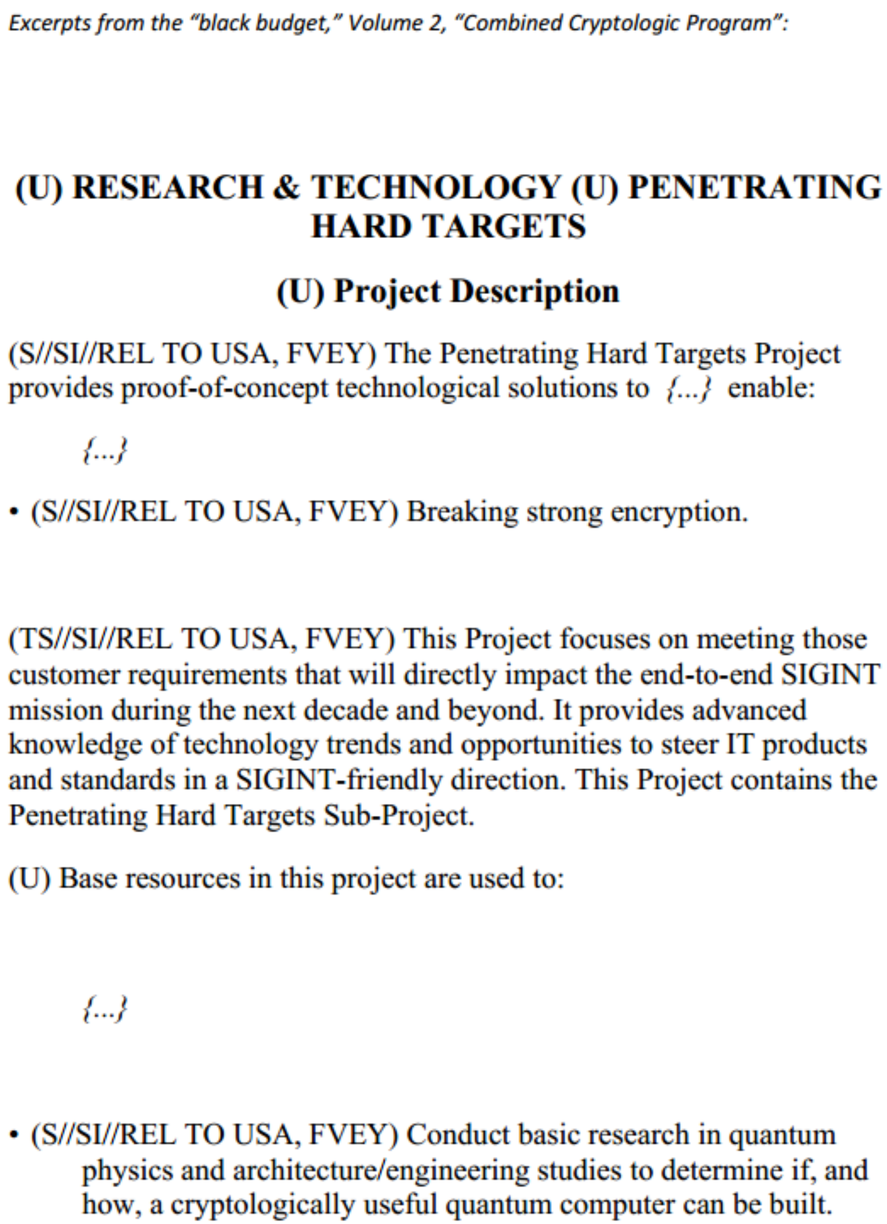
Classical Computing



Quantum Computing

Sometimes, the quantum circuit can be significantly shorter than the classical circuit as in Shor's algorithm that can factor N in polynomial time $O\big((\log N)^3\big)$ whereas the fastest classical factoring algorithm, the general number field sieve works in sub-exponential time $O\left(e^{1.9(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}}\right)$, subsequently breaking public-key cryptography such as RSA and destroying the world as we know it

Tangent



Excerpts from the "black budget," Volume 2, "Combined Cryptologic Program":

(U) RESEARCH & TECHNOLOGY (U) PENETRATING HARD TARGETS

(U) Project Description

(S//SI//REL TO USA, FVEY) The Penetrating Hard Targets Project provides proof-of-concept technological solutions to *{...}* enable:

{...}

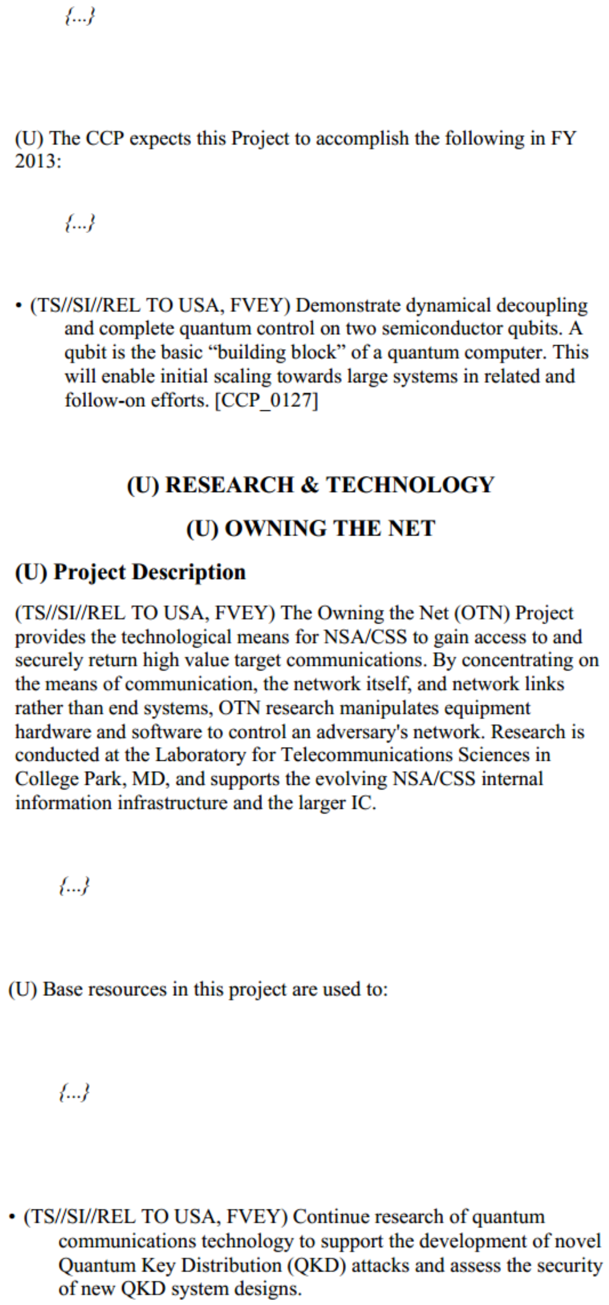
- (S//SI//REL TO USA, FVEY) Breaking strong encryption.

(TS//SI//REL TO USA, FVEY) This Project focuses on meeting those customer requirements that will directly impact the end-to-end SIGINT mission during the next decade and beyond. It provides advanced knowledge of technology trends and opportunities to steer IT products and standards in a SIGINT-friendly direction. This Project contains the Penetrating Hard Targets Sub-Project.

(U) Base resources in this project are used to:

{...}

- (S//SI//REL TO USA, FVEY) Conduct basic research in quantum physics and architecture/engineering studies to determine if, and how, a cryptologically useful quantum computer can be built.



{...}

(U) The CCP expects this Project to accomplish the following in FY 2013:

{...}

- (TS//SI//REL TO USA, FVEY) Demonstrate dynamical decoupling and complete quantum control on two semiconductor qubits. A qubit is the basic "building block" of a quantum computer. This will enable initial scaling towards large systems in related and follow-on efforts. [CCP_0127]

(U) RESEARCH & TECHNOLOGY

(U) OWNING THE NET

(U) Project Description

(TS//SI//REL TO USA, FVEY) The Owning the Net (OTN) Project provides the technological means for NSA/CSS to gain access to and securely return high value target communications. By concentrating on the means of communication, the network itself, and network links rather than end systems, OTN research manipulates equipment hardware and software to control an adversary's network. Research is conducted at the Laboratory for Telecommunications Sciences in College Park, MD, and supports the evolving NSA/CSS internal information infrastructure and the larger IC.

{...}

(U) Base resources in this project are used to:

{...}

- (TS//SI//REL TO USA, FVEY) Continue research of quantum communications technology to support the development of novel Quantum Key Distribution (QKD) attacks and assess the security of new QKD system designs.

Quantum Computing

Bits and Qubits

Quantum Gates

Measurement of Qubits

More Quantum Gates

Universal Computation

Entangled States

Superdense Coding

Measurement Revisited

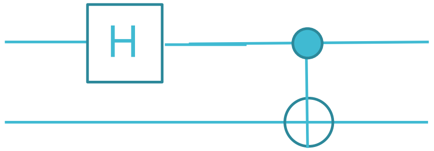
Quantum Teleportation

Surprise?

Entangled States

Entangled states enable quantum computation to be more powerful than classical computation

Entangled States: Intro



$$CNOT(H|00\rangle) \rightarrow CNOT\left(\frac{|00\rangle+|10\rangle}{\sqrt{2}}\right) \rightarrow \frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

$$\frac{|00\rangle+|11\rangle}{\sqrt{2}} \neq (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle) = |\psi\rangle\otimes|\phi\rangle \text{ (non-separable)}$$

Result is a non-classical state, an entangled state, useful for all sorts of things to come; essential difference between a quantum computer from a classical computer

Provable that quantum algorithm without entangled states can be made equivalent to a similarly performant classical algorithm

Entangled States: Intuition

Nobody knows precisely why entangled states are required for performant quantum algorithms

$$|\psi\rangle = \psi_{00\ldots0}|00\ldots0\rangle + \psi_{00\ldots1}|00\ldots1|\rangle + \cdots$$

2^n amplitudes (information) hidden within n qubits

Quantum Computing

Bits and Qubits

Quantum Gates

Measurement of Qubits

More Quantum Gates

Universal Computation

Entangled States

Superdense Coding

Measurement Revisited

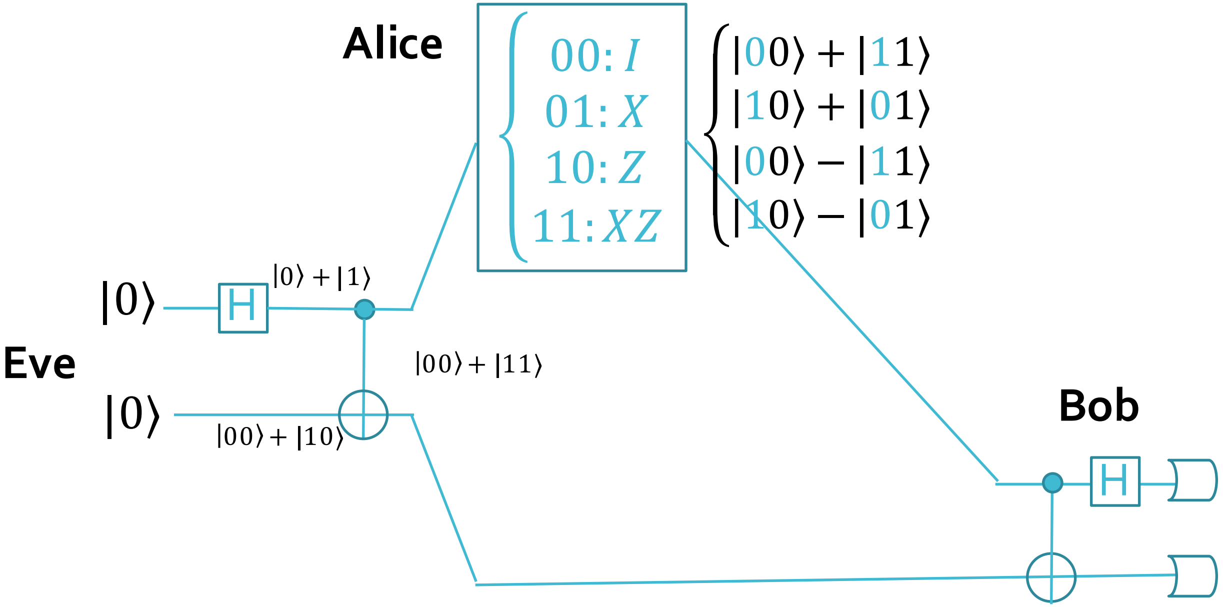
Quantum Teleportation

Surprise?

Superdense Coding

Optimal protocol for equating two classical bits with one qubit

Superdense Coding



$$\begin{cases} 00: I \\ 01: X \\ 10: Z \\ 11: XZ \end{cases}$$

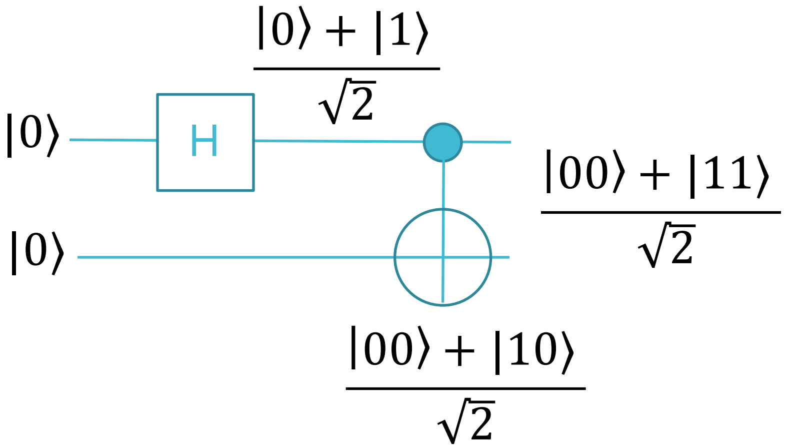
$$\begin{cases} |00\rangle + |11\rangle \\ |10\rangle + |01\rangle \\ |00\rangle - |11\rangle \\ |10\rangle - |01\rangle \end{cases}$$

$$\begin{cases} |00\rangle + |11\rangle \rightarrow |00\rangle + |10\rangle \rightarrow |00\rangle \\ |10\rangle + |01\rangle \rightarrow |11\rangle + |01\rangle \rightarrow |01\rangle \\ |00\rangle - |11\rangle \rightarrow |00\rangle - |10\rangle \rightarrow |10\rangle \\ |10\rangle - |01\rangle \rightarrow |11\rangle - |01\rangle \rightarrow |11\rangle \end{cases}$$

The entangled state that Eve produces enables the protocol

Discovered in 1992 by Charles Bennet and Steven Wiesner (Paper)

Bell State


$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$|0\rangle$
H
$|0\rangle$
$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$
$\frac{|00\rangle + |10\rangle}{\sqrt{2}}$

More generally, for all normalized states $|\psi\rangle$ and $|\phi\rangle$, there exists a unitary U such that $U|\psi\rangle = |\phi\rangle$.

Symbolically,

$\forall\ |\psi\rangle, |\phi\rangle, \exists\ U \mid U|\psi\rangle = |\phi\rangle$

where $\||\psi\rangle\| = 1$ □ $\||\phi\rangle\| = 1$ □ $U^{\dagger}U = I$

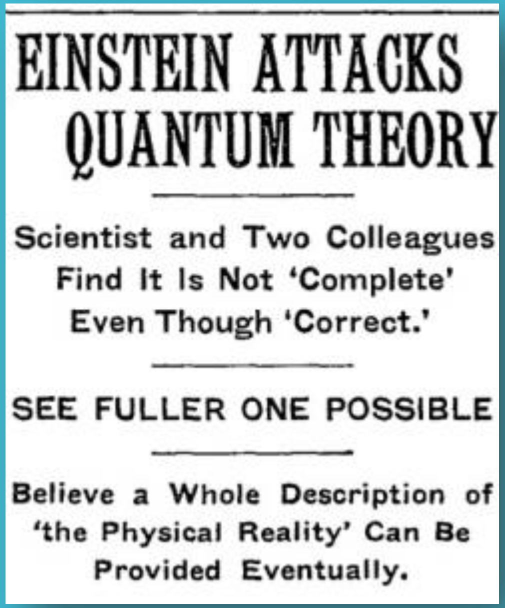
Bell Basis

$$\text{Bell Basis}\begin{cases} \frac{|00\rangle+|11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix} \\ \frac{|10\rangle+|01\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\1\\0\end{bmatrix} \\ \frac{|00\rangle-|11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\-1\end{bmatrix} \\ \frac{|10\rangle-|01\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\-1\\1\\0\end{bmatrix} \end{cases}$$

Orthonomal quantum states and orthogonal normalized quantum states can be distinguished via a unitary function

In each state, determining one bit determines the other

EPR Paradox



EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

"God does not play dice with the Universe" ~ Albert Einstein

Quantum mechanics is an incomplete theory in Einstein's view

Flipping a coin is not random; knowledge of position and momentum degrees of freedom makes it deterministic

Speed of light limits determination of second bit in a bell state

John Bell's Bell Experiment discredits Einstein's hidden local variables theory and supports quantum mechanical probabilities

Quantum Computing

Bits and Qubits

Quantum Gates

Measurement of Qubits

More Quantum Gates

Universal Computation

Entangled States

Superdense Coding

Measurement Revisited

Quantum Teleportation

Surprise?

Measurement Revisited

Generalization of measurement concepts

Measurement in a non-standard basis

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i}\theta}{\sqrt{2}}|1\rangle$$

Standard Orthonormal basis

$$P_\psi(0) = P_\psi(1) = \frac{1}{2}$$

Non-standard $\{|+\rangle, |-\rangle\}$ basis

$$\begin{cases} |+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases} \rightarrow \begin{cases} |0\rangle \equiv \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \\ |1\rangle \equiv \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \end{cases}$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i}\theta}{\sqrt{2}}|1\rangle = \frac{1+e^{i\theta}}{2}|0\rangle + \frac{1-e^{i\theta}}{2}|1\rangle$$

$$\begin{cases} P_\psi(+) = \cos^2\frac{\theta}{2} \\ P_\psi(-) = \sin^2\frac{\theta}{2} \end{cases}$$ from $e^{i\theta} = \cos\theta + i\sin\theta$ (Euler relation)

Measurement in the general orthonormal basis

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

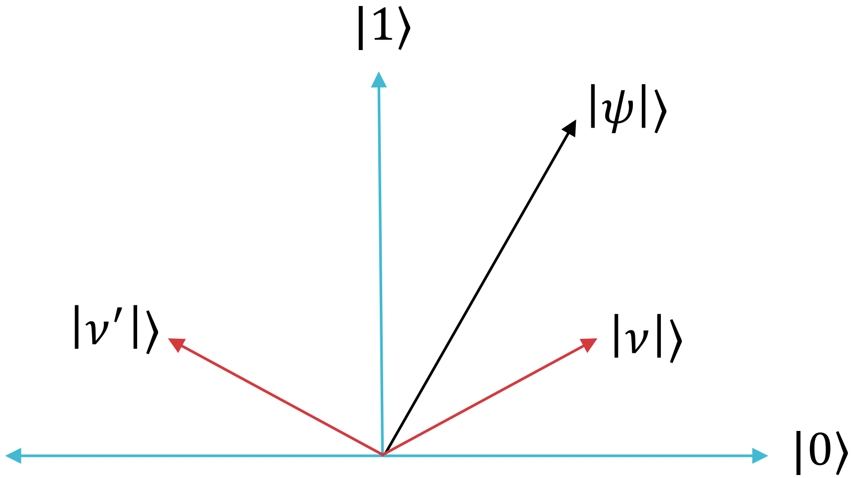
General Orthonormal basis

$$\begin{cases} |\nu\rangle = a|0\rangle + b|1\rangle \\ |\nu'\rangle = b^*|0\rangle - a^*|1\rangle \end{cases}$$

$|\langle\nu|\nu'\rangle| = 0$

$P_\psi(\nu) = |\langle\nu|\psi\rangle|^2 = |a^*\alpha + b^*\beta|^2$

$P_\psi(\nu') = |\langle\nu'|\psi\rangle|^2 = |b\alpha - a\beta|^2$

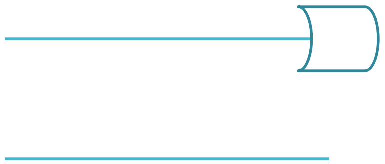


Partial Measurements in the computational basis

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

Measured Qubit

$$P(0) = P(|00\rangle) + P(|01\rangle) = |\alpha|^2 + |\beta|^2$$



Posterior Qubit

$$|\psi\rangle = |0\rangle(\alpha|0\rangle + \beta|1\rangle) + |1\rangle(\gamma|0\rangle + \delta|1\rangle)$$

$$|\psi\rangle = \left(\frac{\alpha|0\rangle+\beta|1\rangle}{\sqrt{|\alpha|^2+|\beta|^2}}\right)$$

Quantum Computing

Bits and Qubits

Quantum Gates

Measurement of Qubits

More Quantum Gates

Universal Computation

Entangled States

Superdense Coding

Measurement Revisited

Quantum Teleportation

Surprise?

Quantum Teleportation

Cloning quantum state with two classical bits

Quantum Teleportation: Problem

$$\begin{gathered}P(We\ have\ time\ for\ this) = \\ P(I\ will\ ever\ understand\ any\ of\ this) = 0\end{gathered}$$

Google and NASA's Quantum Artificial Intelligence Lab

October 11, 2013