Quantum Information Science

양자정보과학

量子情報科學

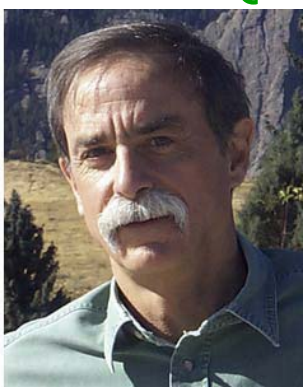
信息

資訊

고등과학원 계산과학부
김재완 (jaewan@kias.re.kr)

Some stuffs are from Nielsen and Chuang's book
"Quantum computation and quantum information"

MEASURING AND MANIPULATING INDIVIDUAL QUANTUM SYSTEMS



THE LAUREATES

SERGE HAROCHE
French citizen. Born 1944 in Casablanca, Morocco. Ph.D. 1971 from Universite Pierre et Marie Curie, Paris, France. Professor at College de France and Ecole
Normale Superieure, Paris, France.
www.college-de-france.fr/site/en-serge-haroche/biography.htm

DAVID J. WINELAND
U.S. citizen. Born 1944 in Milwaukee, WI, USA. Ph.D. 1970 from Harvard University, Cambridge, MA, USA. Group Leader and NIST Fellow at National Institute of Standards and Technology (NIST) and University of Colorado Boulder, CO, USA.
www.nist.gov/pml/div688/grp10/index.cfm

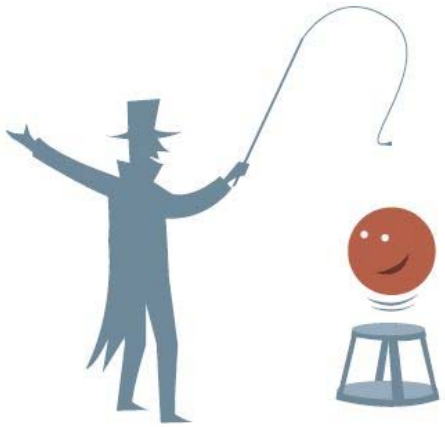


Figure 1. Nobel Prize awarded for mastering particles. The Laureates have managed to make trapped, individual particles to behave according to the rules of quantum physics.

Ion Trap

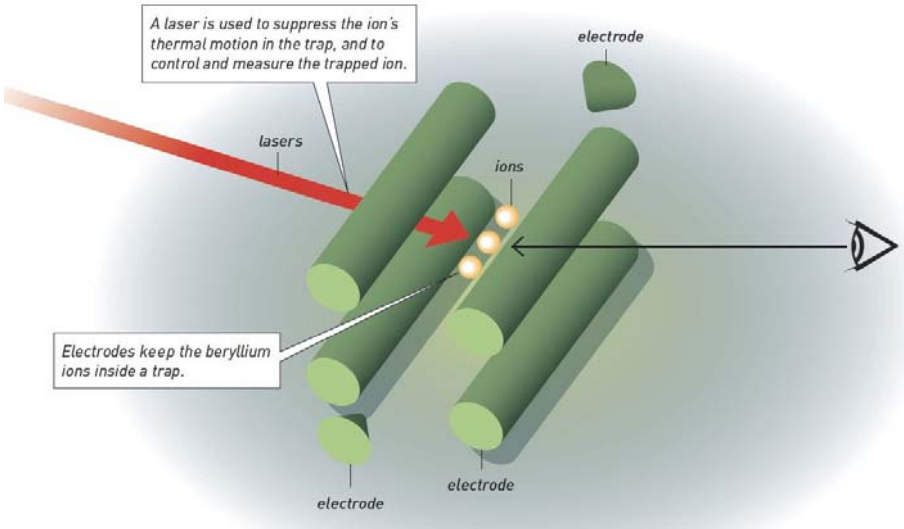


Figure 2. In David Wineland's laboratory in Boulder, Colorado, electrically charged atoms or ions are kept inside a trap by surrounding electric fields. One of the secrets behind Wineland's breakthrough is mastery of the art of using laser beams and creating laser pulses. A laser is used to put the ion in its lowest energy state and thus enabling the study of quantum phenomena with the trapped ion.

Manipulate charged atom(ion) by light(laser)

Cavity Quantum ElectroDynamics

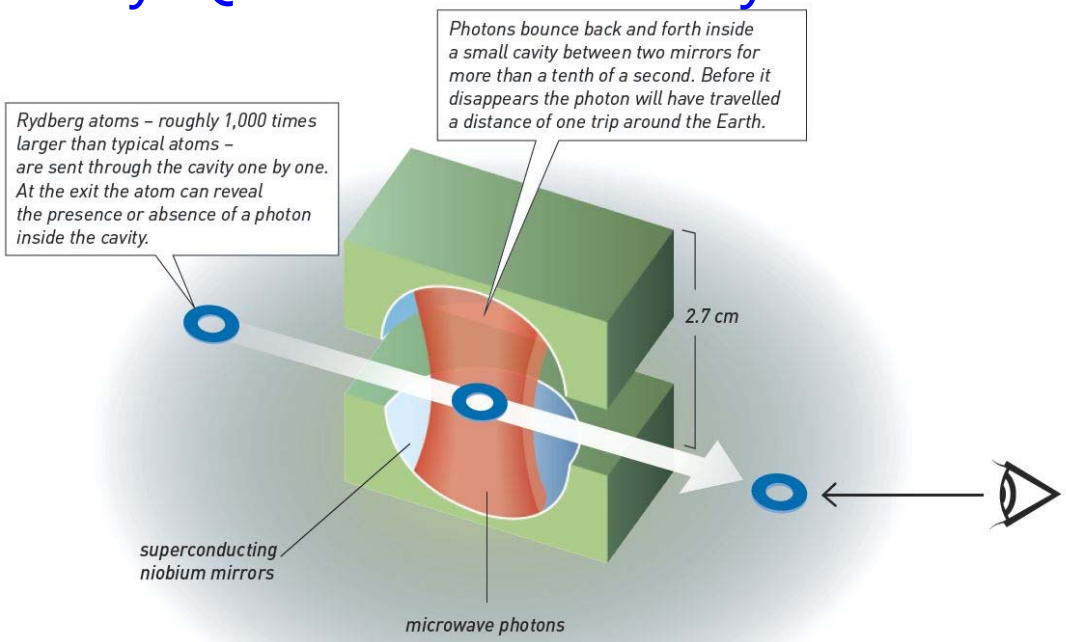
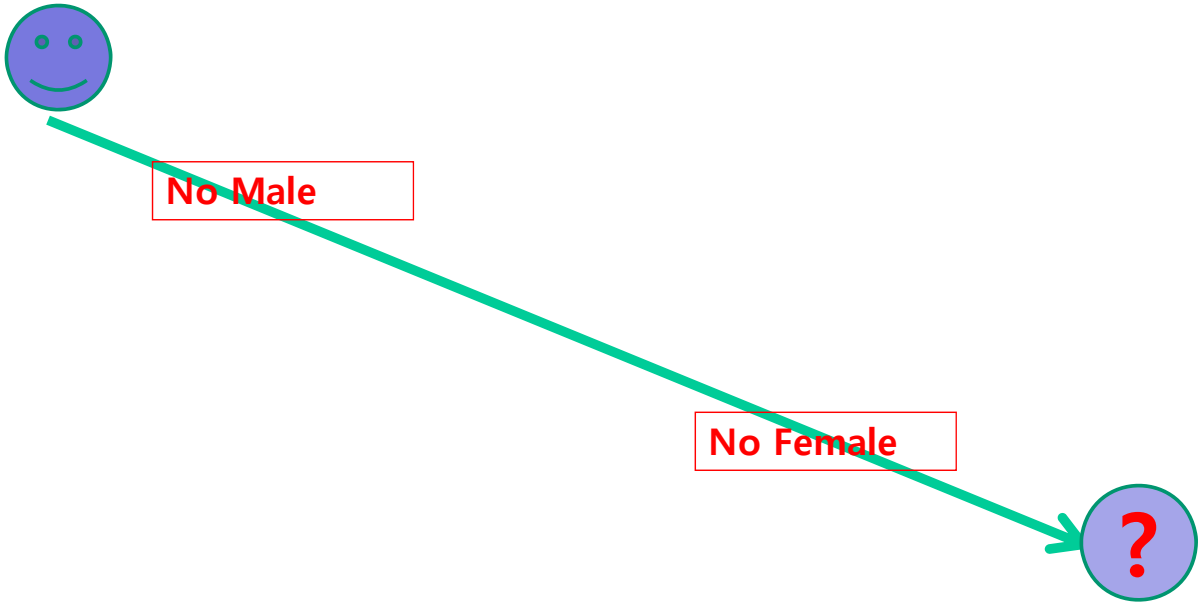


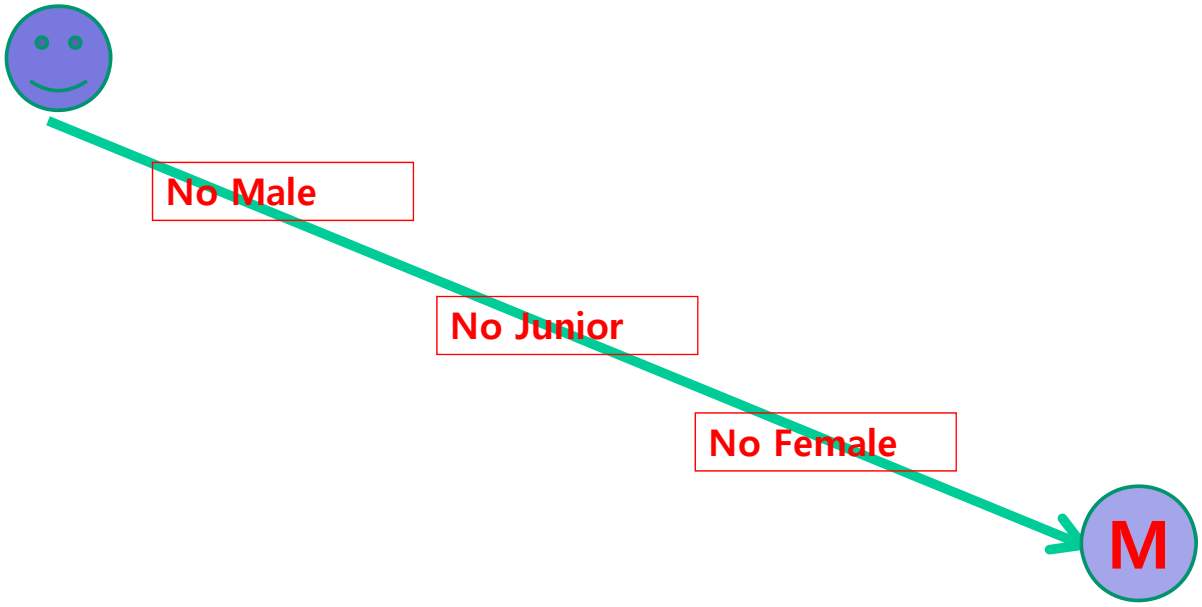
Figure 3. In the Serge Haroche laboratory in Paris, in vacuum and at a temperature of almost absolute zero, the microwave photons bounce back and forth inside a small cavity between two mirrors. The mirrors are so reflective that a single photon stays for more than a tenth of a second before it is lost. During its long life time, many quantum manipulations can be performed with the trapped photon without destroying it.

Measure light trapped between two mirrors by atoms

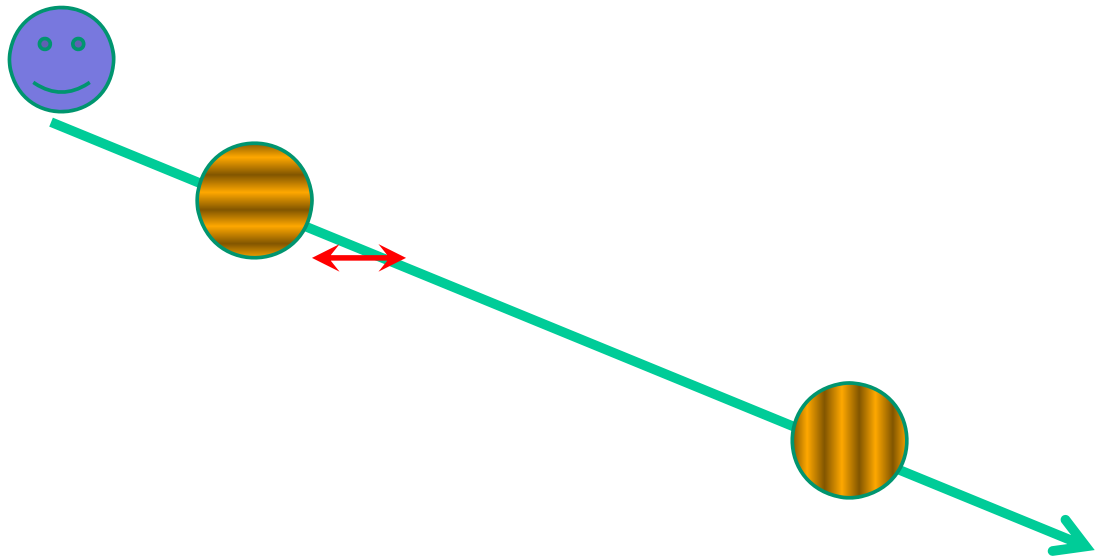
M/F; S/J



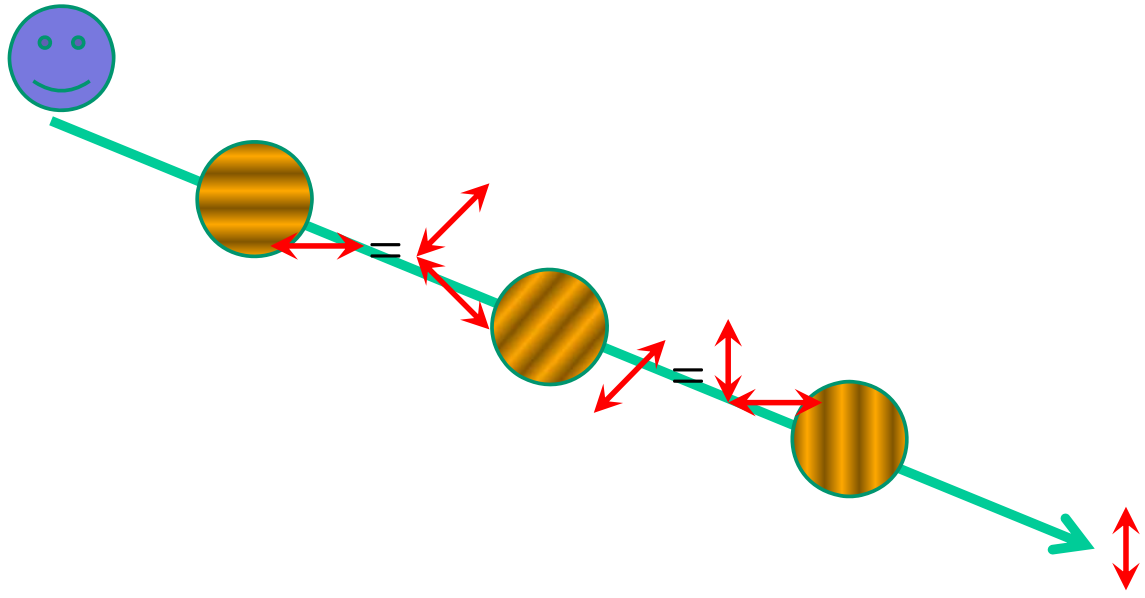
M/F; S/J



M/F; S/J ➔ Polarization



M/F; S/J ➔ Polarization



Quantum Beyond Nano

"There's plenty of room at the bottom." -Feynman
Moore's Law :continue to shrink→ nanotechnology
→ meets quantum regime
→ uncertainty principle
uncertainty in bits (0's and 1's)

Quantum Technology
→ turns uncertainty into magic
Actively *utilizing quantumness*
'Let the quantum system solve
the quantum manybody problems' -Feynman

I think of my lifetime in physics as divided into three periods.

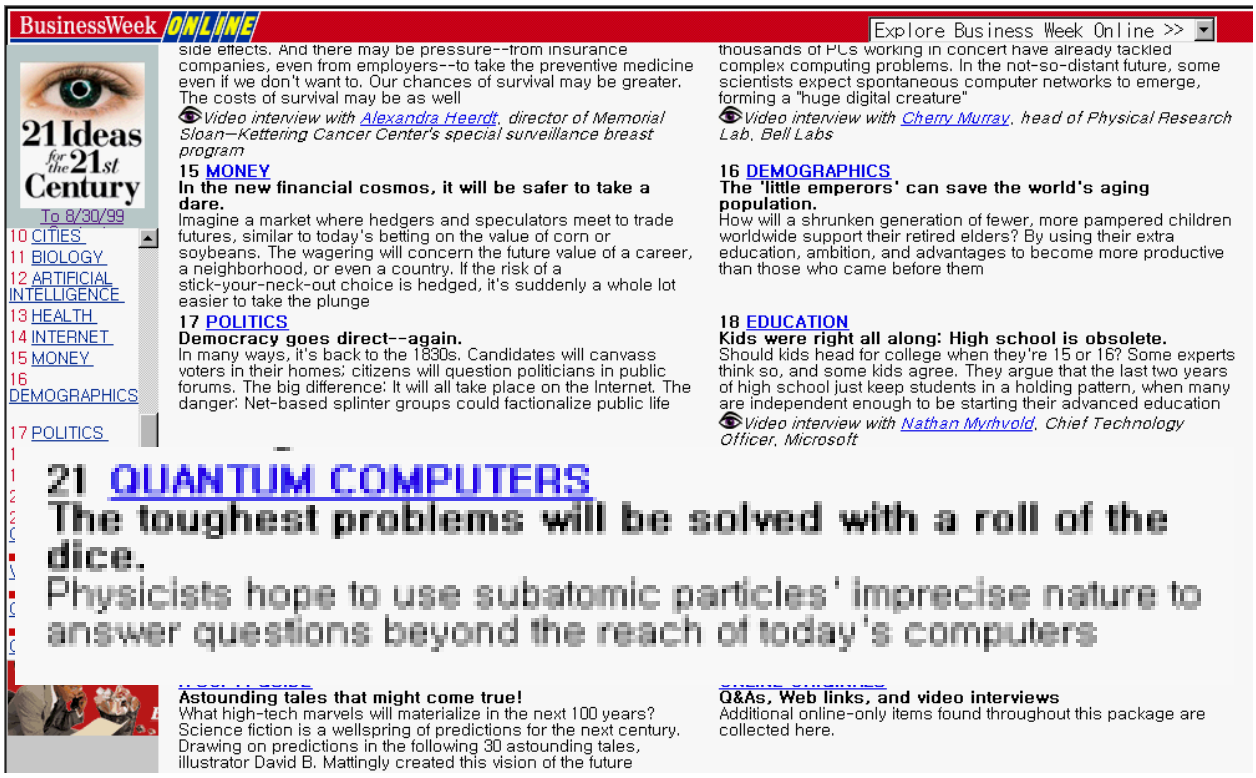
In the first period … I was in the grip of the idea that Everything is Particles, …

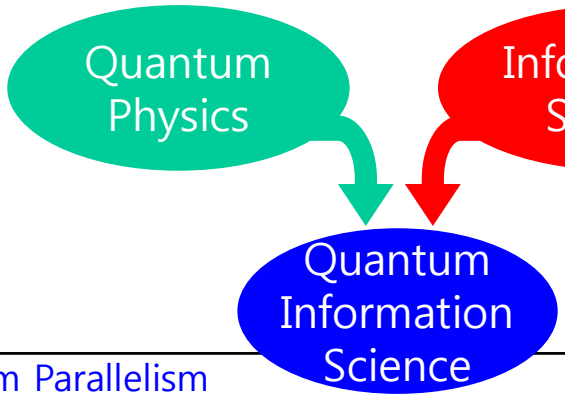
I call my second period Everything is Fields.
…

Now I am in the grip of a new vision, that
Everything is Information.

– John Archibald Wheeler, *Geon, Black Holes, and Quantum Foam* –

Businessweek 21 Ideas for the 21st Century





Quantum Parallelism

→ Quantum computing is exponentially larger and faster than digital computing.
Quantum Fourier Transform, Quantum Database Search,
Quantum Many-Body Simulation (Nanotechnology)

No Clonability of Quantum Information,
Irrevesability of Quantum Measurement

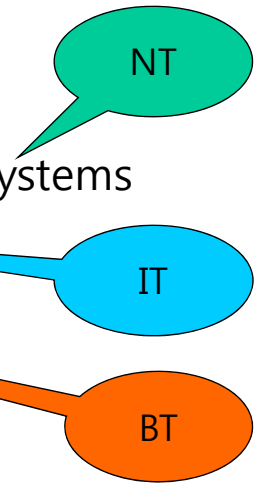
→ Quantum Cryptography (Absolutely secure digital communication)

Quantum Correlation by Quantum Entanglement

→ Quantum Teleportation, Quantum Superdense Coding,
Quantum Cryptography, Quantum Imaging

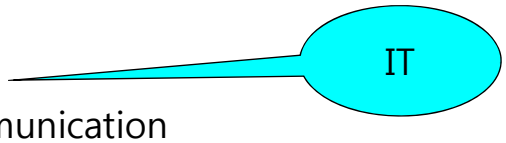
Quantum Information Processing

- Quantum Computer
  - Quantum Algorithms: Softwares
    - Simulation of quantum many-body systems
    - Factoring large integers
    - Database search
  - Experiments: Hardwares
    - Ion Traps
    - NMR
    - Cavity QED
    - Quantum optics
    - Superconducting qubits, etc.

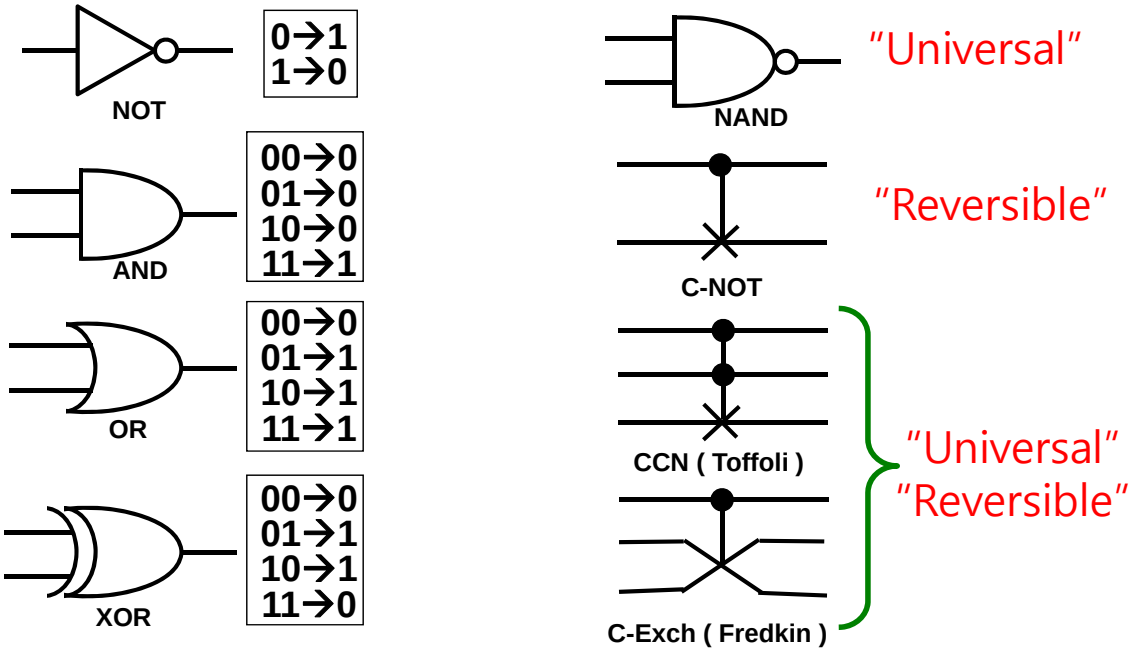


Quantum Information Processing

- Quantum Communication
  - Quantum Cryptography
    - Absolutely secure digital communication
    - Generation and Distribution of Quantum Key
      - optical fiber
      - wireless→ secure satellite communication
  - Quantum Teleportation
    - Photons
    - Atoms, Molecules
- Quantum Imaging and Quantum Metrology



Bit and Logic Gate

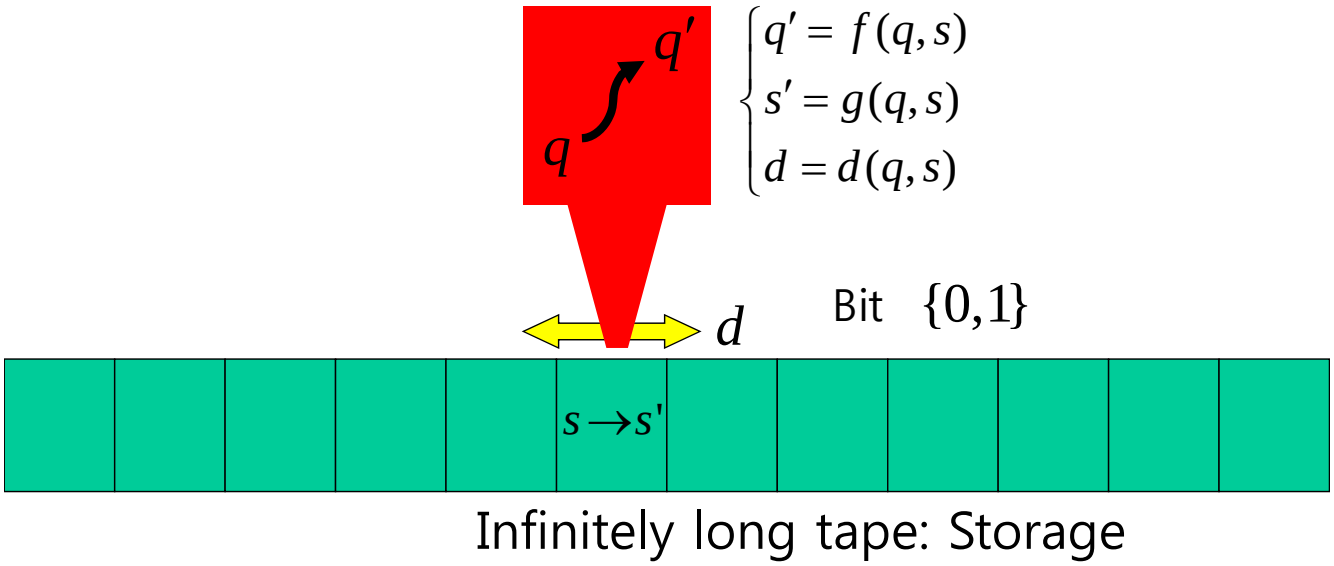


Classical Computation

- Hilbert (1900): 23 most challenging math problems
  - Is there a mechanical procedure by which the truth or falsity of any mathematical conjecture could be decided?
- Turing
  - Conjecture ~ Sequence of 0's and 1's
  - Read/Write Head: Logic Gates
  - Model of Modern Computers

Turing Machine

Finite State Machine: Head



Infinitely long tape: Storage

Quantum Information

- Bit $\{0,1\}$ ➔ Qubit $a|0\rangle + b|1\rangle$ with $|a|^2 + |b|^2 = 1$
- N bits $\Rightarrow$ 2^N states, One at a time

  Linearly parallel computing AT BEST
- N qubits ➔ Linear superposition

  of 2^N states at the same time

  Exponentially parallel computing

  ➔ Quantum Parallelism Deutsch

But when you extract result,

you cannot get all of them.

Quantum Algorithms

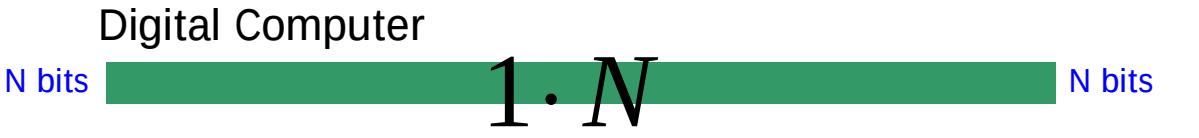
1. [Feynman] Simulation of Quantum Physical Systems with HUGE Hilber space (2^N-D)
   e.g. Strongly Correlated Electron Systems

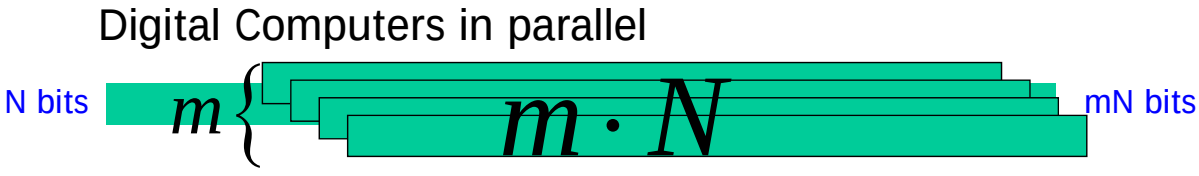
2. [Peter Shor] Factoring large integers, period finding

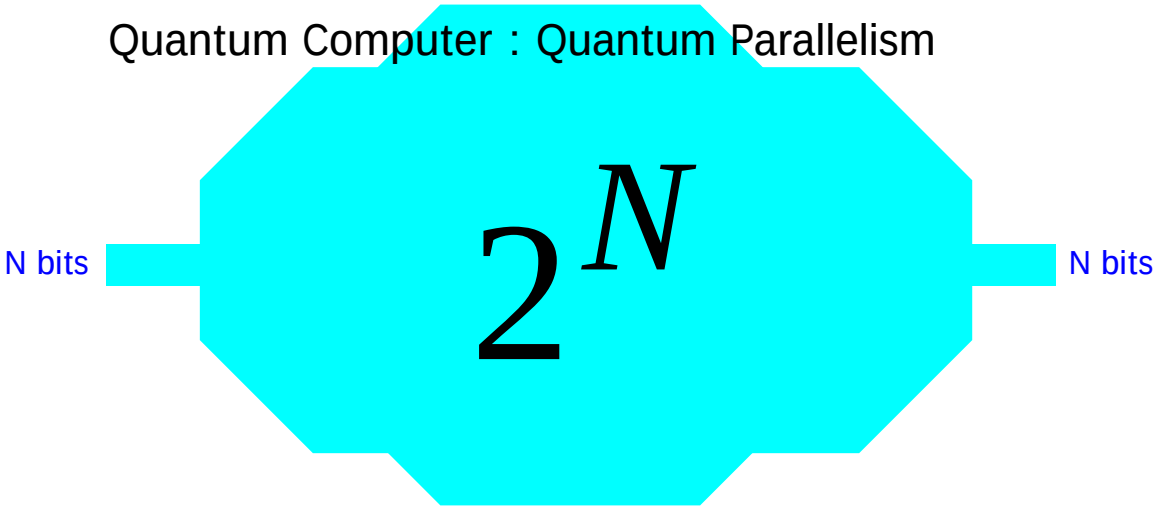
   $t_q \propto$ Pol (N) $t_{cl} \sim$ Exp ($N^{1/3}$)

3. [Grover] Searching

   $t_q \propto \sqrt{N}$ $\langle t_{cl} \rangle \sim N/2$







Quantum Gates

Time-dependent Schrödinger Eq.

$$i\hbar\frac{\partial}{\partial t}|\psi\rangle = H|\psi\rangle$$

$$|\psi(t)\rangle = e^{-iHt/\hbar}|\psi(0)\rangle = U(t)|\psi(0)\rangle$$

Unitary Transform
Norm Preserving
Reversible

$$P(\theta)=\begin{pmatrix}1 & 0\\ 0 & e^{i\theta}\end{pmatrix}\quad I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\quad X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

$$Z=\mathrm{P}(\pi)=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\quad Y=XZ=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\quad H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

Hadamard

$$H|0\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix}=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$$

$$H|1\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix}=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

Hadamard Gate

$$H_1\otimes H_2\otimes\ldots\otimes H_N|0\rangle_1\otimes|0\rangle_2\otimes\ldots\otimes|0\rangle_N$$

$$=\frac{1}{\sqrt{2}}\left(|0\rangle_1+|1\rangle_1\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle_2+|1\rangle_2\right)\otimes\ldots\frac{1}{\sqrt{2}}\left(|0\rangle_N+|1\rangle_N\right)$$

$$=\frac{1}{\sqrt{2^N}}\left(|0_1 0_2\ldots 0_N\rangle+|1_1 0_2\ldots 0_N\rangle+\ldots+|1_1 1_2\ldots 1_N\rangle\right)$$

$$=\frac{1}{\sqrt{2^N}}\sum_{k=0}^{2^{N-1}}|k(\text{binary expression})\rangle$$

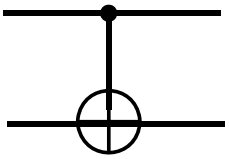
Universal Quantum Gates

General Rotation of a Single Qubit

$$V(\theta,\phi)=\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -ie^{-i\phi}\sin\left(\frac{\theta}{2}\right) \\ -ie^{+i\phi}\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

X_c: CNOT (controlled - NOT) or XOR

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\otimes\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}+\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\otimes\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$=|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes X$$



$$X_c|a\rangle|b\rangle=|a\rangle|a\oplus b\rangle$$

Hadamard	H	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli-X	X	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y	Y	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z	Z	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase	S	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$	T	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

controlled-NOT

$CNOT = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$

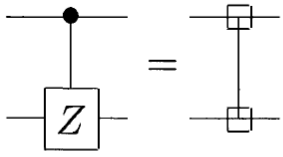
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

swap

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

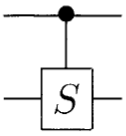
controlled-Z

$CZ = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$



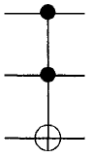
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

controlled-phase



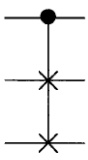
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$$

Toffoli

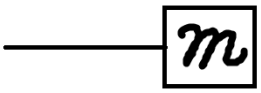


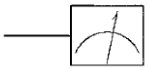
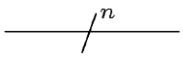
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Fredkin (controlled-swap)



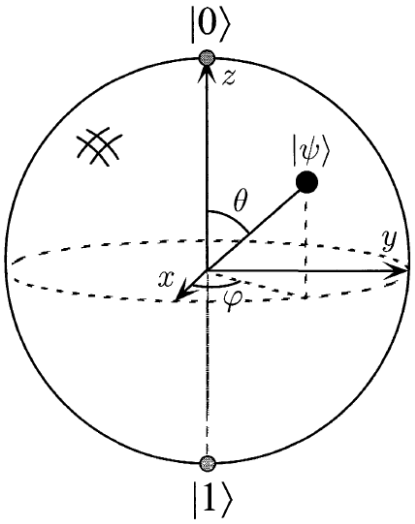
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$



measurement		Projection onto $\|0\rangle$ and $\|1\rangle$
qubit		wire carrying a single qubit (time goes left to right)
classical bit		wire carrying a single classical bit
n qubits		wire carrying n qubits

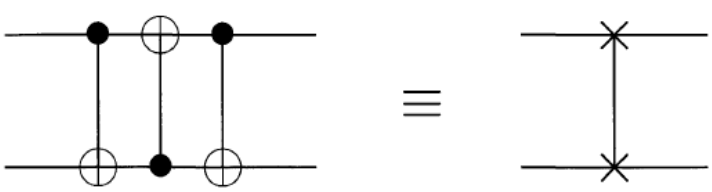
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \qquad |\alpha|^2 + |\beta|^2 = 1$$

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$$



Bloch sphere representation of a qubit

$$U = e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix}, \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix}$$



$$\begin{aligned} |a, b\rangle &\longrightarrow |a, a \oplus b\rangle \\ &\longrightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \\ &\longrightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle \,, \end{aligned}$$

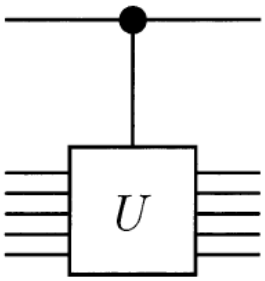
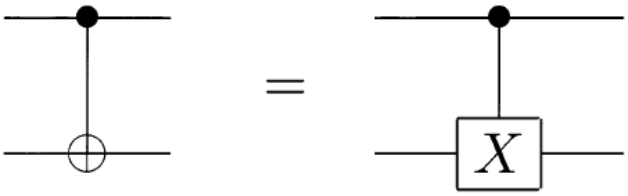
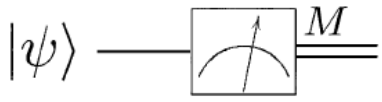
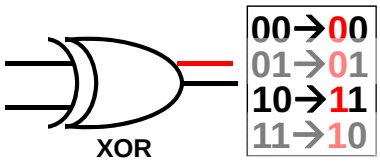


Figure 1.8. Controlled-U gate.

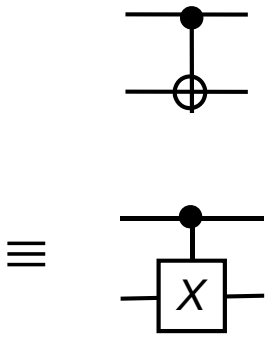






$$X_{AB} = |0\rangle_{AA}\langle 0| \otimes I_B + |1\rangle_{AA}\langle 1| \otimes X_B$$

Controlled-NOT

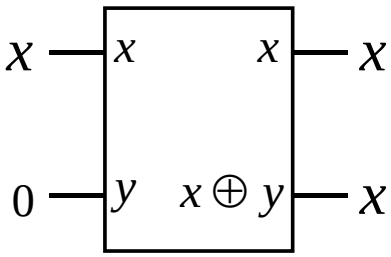


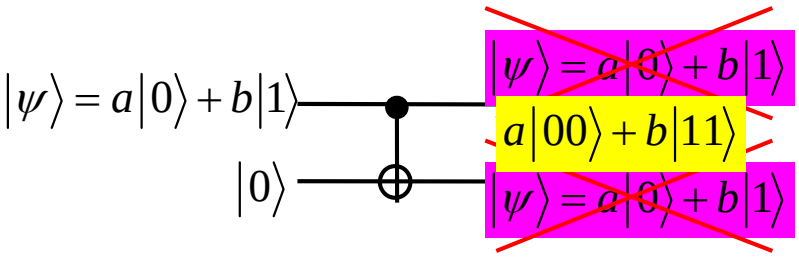
$$= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}_A \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}_B + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}_A \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}_B$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}_{AB} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{AB}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{AB}$$

Qubit Copying Circuit?





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

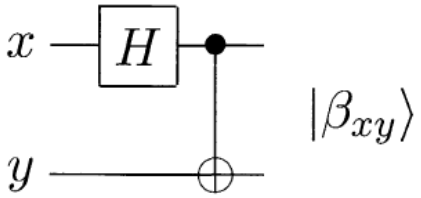
$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

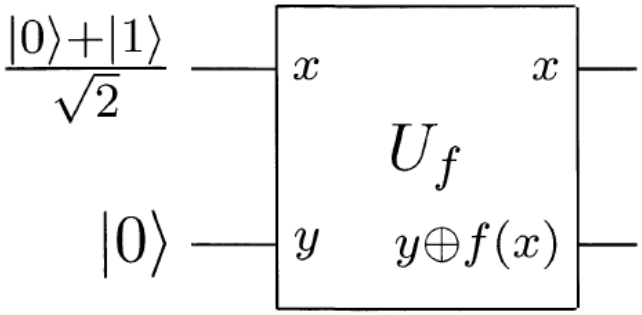
$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

$$|\beta_{xy}\rangle \equiv \frac{|0, y\rangle + (-1)^x |1, \bar{y}\rangle}{\sqrt{2}}$$

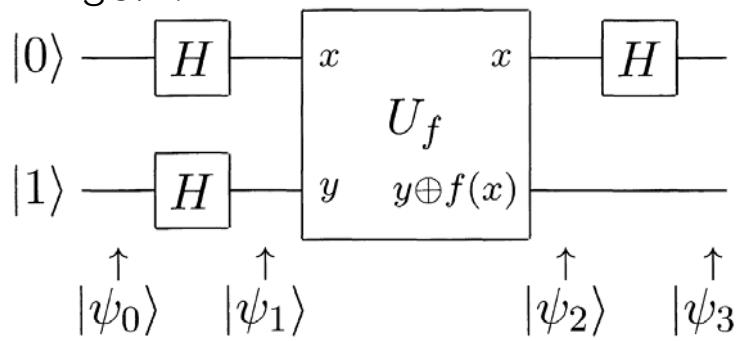
In	Out
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} \equiv \|\beta_{11}\rangle$





$$|\psi\rangle = \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

Deutsch Algorithm



$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1). \end{cases}$$

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1). \end{cases} = \pm|f(0) \oplus f(1)\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Global property of f

Notation	Description
z^*	Complex conjugate of the complex number z. $(1+i)^* = 1 - i$
$\|\psi\rangle$	Vector. Also known as a *ket*.
$\langle\psi\|$	Vector dual to $\|\psi\rangle$. Also known as a *bra*.
$\langle\varphi\|\psi\rangle$	Inner product between the vectors $\|\varphi\rangle$ and $\|\psi\rangle$.
$\|\varphi\rangle \otimes \|\psi\rangle$	Tensor product of $\|\varphi\rangle$ and $\|\psi\rangle$.
$\|\varphi\rangle\|\psi\rangle$	Abbreviated notation for tensor product of $\|\varphi\rangle$ and $\|\psi\rangle$.
A^*	Complex conjugate of the A matrix.
A^T	Transpose of the A matrix.
$A^\dagger$	Hermitian conjugate or adjoint of the A matrix, $A^\dagger = (A^T)^*$. $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$.
$\langle\varphi\|A\|\psi\rangle$	Inner product between $\|\varphi\rangle$ and $A\|\psi\rangle$. Equivalently, inner product between $A^\dagger\|\varphi\rangle$ and $\|\psi\rangle$.

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\langle v|w\rangle = \left(\sum_i v_i|i\rangle, \sum_j w_j|j\rangle\right) = \sum_{ij} v_i^* w_j \delta_{ij} = \sum_i v_i^* w_i$$

$$= \begin{bmatrix} v_1^* \dots v_n^* \end{bmatrix} \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}.$$

$$\sum_i |i\rangle\langle i| = I$$

$$A \otimes B \equiv \overbrace{\begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix}}^{nq} \Bigg\} mp$$

$$\exp(i\theta\vec{v}\cdot\vec{\sigma}) = \cos(\theta)I + i\sin(\theta)\vec{v}\cdot\vec{\sigma},$$

$$\mathrm{tr}(A) \equiv \sum_i A_{ii}$$

The Hilbert–Schmidt inner product on operators

$$(A, B) \equiv \mathrm{tr}(A^\dagger B)$$

$$[A, B] \equiv AB - BA \qquad \{A, B\} \equiv AB + BA$$

$$[X, Y] = 2iZ; \quad [Y, Z] = 2iX; \quad [Z, X] = 2iY.$$

$$[\sigma_j, \sigma_k] = 2i \sum_{l=1}^{3} \epsilon_{jkl} \sigma_l$$

$$\{\sigma_i, \sigma_j\} = 0 \quad \text{where } i \neq j$$

$$\sigma_i^2 = I$$

$$\sigma_j \sigma_k = \delta_{jk} I + i \sum_{l=1}^{3} \epsilon_{jkl} \sigma_l$$

Theorem 2.3: (**Polar decomposition**) Let A be a linear operator on a vector space V. Then there exists unitary U and positive operators J and K such that

$$A = UJ = KU, \tag{2.79}$$

where the unique positive operators J and K satisfying these equations are defined by $J \equiv \sqrt{A^\dagger A}$ and $K \equiv \sqrt{AA^\dagger}$. Moreover, if A is invertible then U is unique.

Corollary 2.4: (**Singular value decomposition**) Let A be a square matrix. Then there exist unitary matrices U and V, and a diagonal matrix D with non-negative entries such that

$$A = UDV\,. \tag{2.80}$$

The diagonal elements of D are called the *singular values* of A.

Proof

By the polar decomposition, $A = SJ$, for unitary S, and positive J. By the spectral theorem, $J = TDT^\dagger$, for unitary T and diagonal D with non-negative entries. Setting $U \equiv ST$ and $V \equiv T^\dagger$ completes the proof. □

Theorem 2.7: (**Schmidt decomposition**) Suppose $|\psi\rangle$ is a pure state of a composite system, AB. Then there exist orthonormal states $|i_A\rangle$ for system A, and orthonormal states $|i_B\rangle$ of system B such that

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle, \tag{2.202}$$

where λ_i are non-negative real numbers satisfying $\sum_i \lambda_i^2 = 1$ known as *Schmidt co-efficients*.

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}.$$

$$R_{\hat{n}}(\theta) \equiv \exp(-i\theta\, \hat{n}\cdot\vec{\sigma}/2) = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) (n_x X + n_y Y + n_z Z)$$

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

$$U = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2} \end{bmatrix}$$

Corollary 4.2: Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and $U = e^{i\alpha} AXBXC$, where α is some overall phase factor.

Proof

In the notation of Theorem 4.1, set $A \equiv R_z(\beta)R_y(\gamma/2)$, $B \equiv R_y(-\gamma/2)R_z(-(\delta+\beta)/2)$ and $C \equiv R_z((\delta-\beta)/2)$. Note that

$$ABC = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(-\frac{\gamma}{2}\right)R_z\left(-\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) = I\,. \tag{4.14}$$

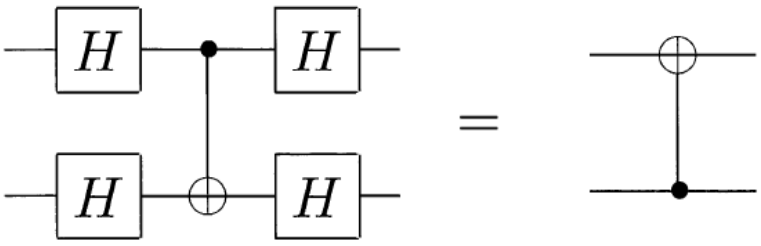
Since $X^2 = I$, and using Exercise 4.7, we see that

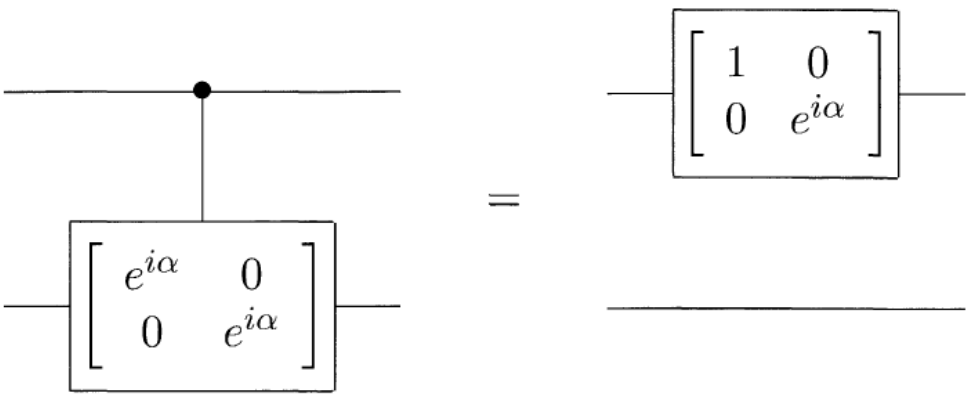
$$XBX = XR_y\left(-\frac{\gamma}{2}\right)XXR_z\left(-\frac{\delta+\beta}{2}\right)X = R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right). \tag{4.15}$$

Thus

$$AXBXC = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) \tag{4.16}$$

$$= R_z(\beta)R_y(\gamma)R_z(\delta)\,. \tag{4.17}$$





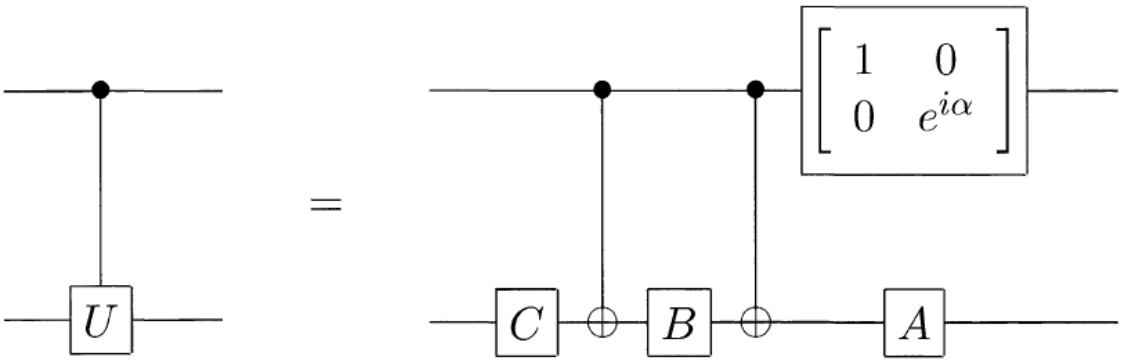


Figure 4.6. Circuit implementing the controlled-U operation for single qubit U. α, A, B and C satisfy $U = \exp(i\alpha)AXBXC$, $ABC = I$.

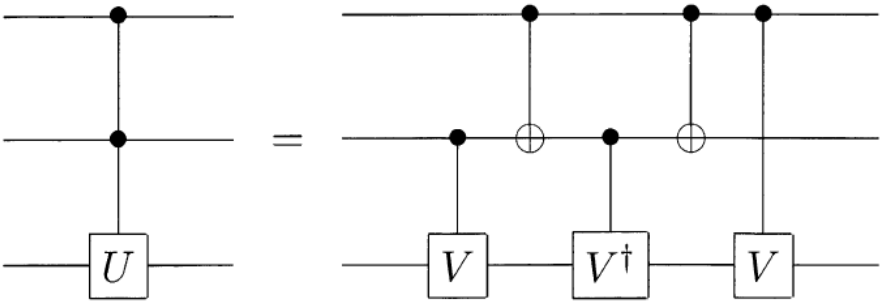


Figure 4.8. Circuit for the $C^2(U)$ gate. V is any unitary operator satisfying $V^2 = U$. The special case $V \equiv (1-i)(I+iX)/2$ corresponds to the Toffoli gate.

Quantum Fourier Transform

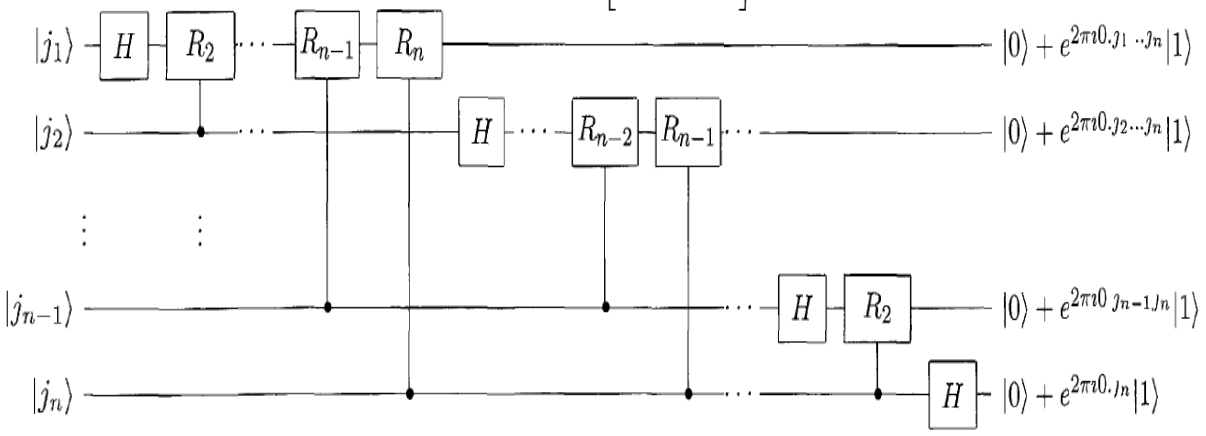
$$\sum_{j=0}^{2^n-1} x_j |j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left[\sum_{j=0}^{2^n-1} e^{2\pi i j k/2^n} x_j \right] |k\rangle = \sum_{k=0}^{2^n-1} y_k |k\rangle$$

$$\begin{aligned}
|j\rangle &\longrightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k/2^n} |k\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j \left(\sum_{l=1}^{n} k_l 2^{-l}\right)} |k_1 \ldots k_n\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \\
&= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right] \\
&= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + 2^{2\pi i j 2^{-l}} |1\rangle \right] \\
&= \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)}{2^{n/2}}
\end{aligned}$$

Quantum Fourier Transform

$$\frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2 \ldots j_n}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)$$

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$



~$n^2=(\log_2 N)^2$ vs $N \log_2 N$

***can be used only as a subroutine, used for factoring

Grover Search

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle$$

$$\begin{cases} f(x) = 1 \\ f(k) = 0 \text{ for } k \neq x \end{cases}$$

$$\hat{O}|\psi\rangle|-\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (-1)^{f(k)} |k\rangle|-\rangle$$

$$\hat{D} = 2|\psi\rangle\langle\psi| - \hat{I}$$

$$\hat{G} \equiv \hat{D}\hat{O}$$

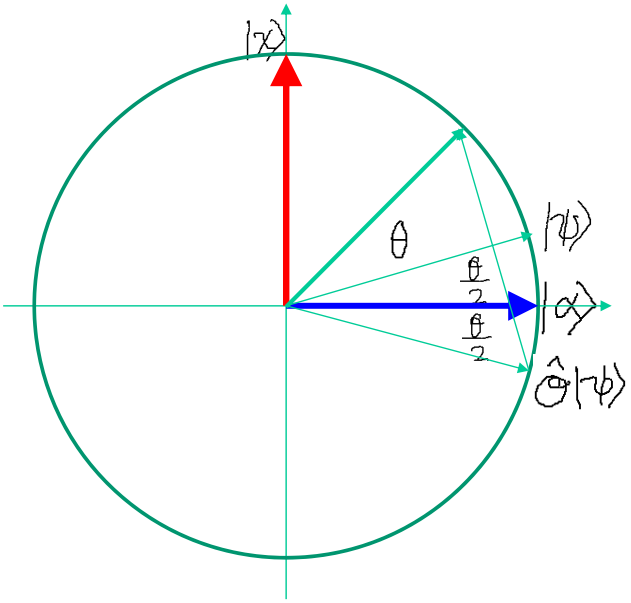
$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum'' |k'\rangle + \frac{1}{\sqrt{2^n}}|x\rangle$$
$$= \sqrt{\frac{N-1}{N}}|\alpha\rangle + \frac{1}{\sqrt{N}}|x\rangle$$

$$\hat{G}|\psi\rangle = (2|\psi\rangle\langle\psi| - \hat{I})\hat{O}|\psi\rangle$$
$$= (2|\psi\rangle\langle\psi| - \hat{I})\left\{\underbrace{\sqrt{\frac{N-1}{N}}}_{\cos\frac{\theta}{2}}|\alpha\rangle - \underbrace{\frac{1}{\sqrt{N}}}_{\sin\frac{\theta}{2}}|x\rangle\right\}$$

Grover Search

$$\hat{G}|\psi\rangle = \left(2|\psi\rangle\langle\psi| - \hat{I}\right)\hat{\theta}|\psi\rangle$$

$$= \left(2|\psi\rangle\langle\psi| - \hat{I}\right)\left\{\underbrace{\sqrt{\frac{N-1}{N}}}_{\cos\frac{\theta}{2}}|\alpha\rangle - \underbrace{\frac{1}{\sqrt{N}}}_{\sin\frac{\theta}{2}}|\chi\rangle\right\}$$



$$\sin\frac{\theta}{2} = \frac{1}{\sqrt{N}} \Rightarrow \theta \simeq \frac{2}{\sqrt{N}}$$

$$\frac{\pi/2}{\theta} \simeq \frac{\pi}{2\theta} = \frac{\pi}{4}\sqrt{N}$$

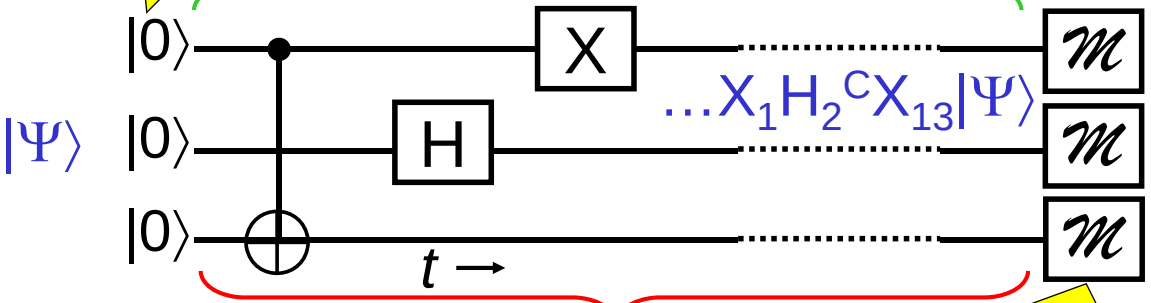
Quantum Network

DiVincenzo, Qu-Ph/0002077

Scalable Qubits

Initial State

Unitary evolution
: Deterministic
: Reversible
Universal Gates



Cohere,
Not Decohere

Quantum measurement
: Probabilistic
: Irreversible change

Quantum Key Distribution √ [BB84,B92]	Single-Qubit Gates	~ 3
QKD[E91] √ Quantum Repeater Quantum Teleportation √	Single- & Two-Qubit Gates	~ 3
Quantum Error Correction Quantum Computer 10-Qubit QC √	Single- & Two-Qubit Gates	≫ 100

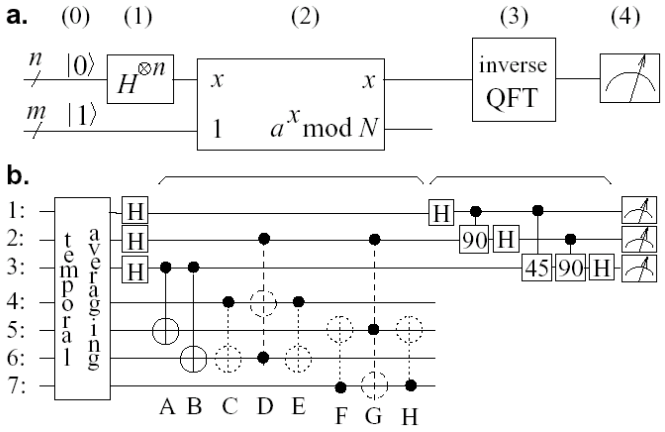
Physical systems actively considered for quantum computer implementation

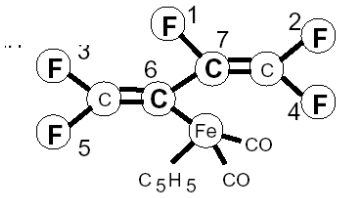
- Liquid-state NMR
- NMR spin lattices
- Linear ion-trap spectroscopy
- Neutral-atom optical lattices
- Cavity QED + atoms
- Linear optics with single photons
- Nitrogen vacancies in diamond
- Electrons on liquid He
- Superconducting Qubits; Josephson junctions
  - "charge" qubits
  - "flux" qubits
- Spin spectroscopies, impurities in semiconductors
- Coupled quantum dots
  - Qubits: spin,charge, excitons
  - Exchange coupled, cavity coupled

$15 = 3 \times 5$

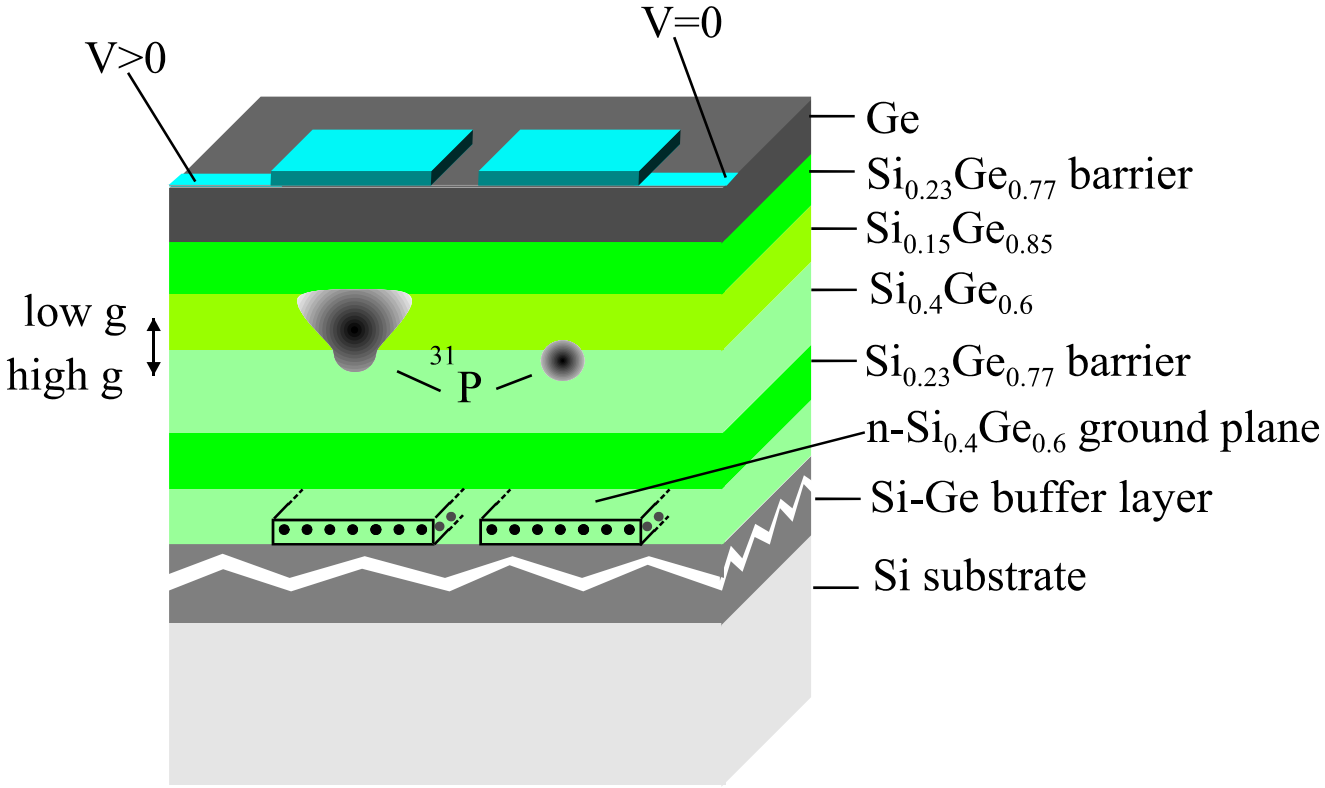
Chuang

Nature 414, 883-887 (20/27 Dec 2001)
OR QP/0112176



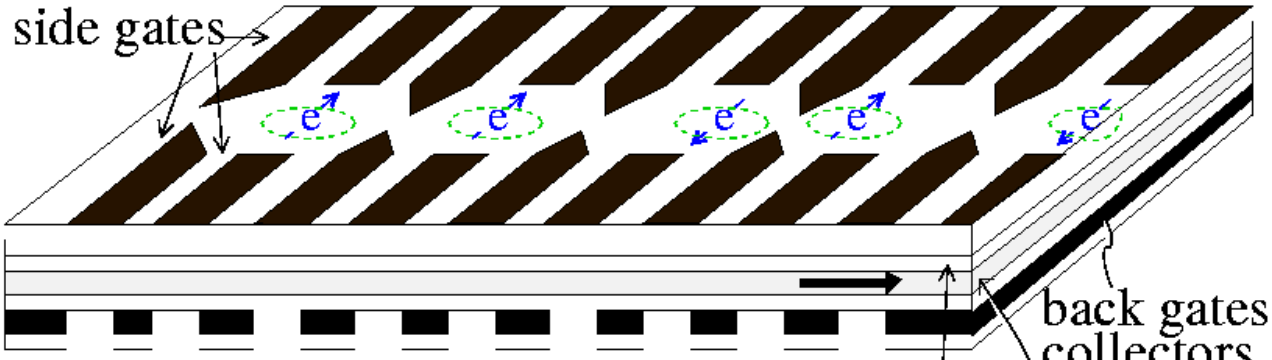


Concept device: spin-resonance transistor
R. Vrijen et al, Phys. Rev. A 62, 012306 (2000)



Quantum–dot array proposal:

Loss & DiVincenzo, Phys. Rev. A 57, 120 (1998).



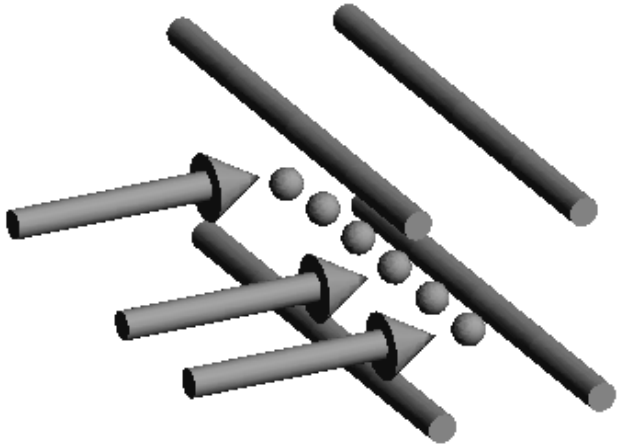
–quantum dots defined in 2DEG by side gates
–Coulomb blockade used to fix electron number at one per dot
–spin of electron is qubit
–gate operations: controllable coupling of dots by point–contact gate voltage
–readout by gatable magnetic barrier

Quantum–dot array proposal

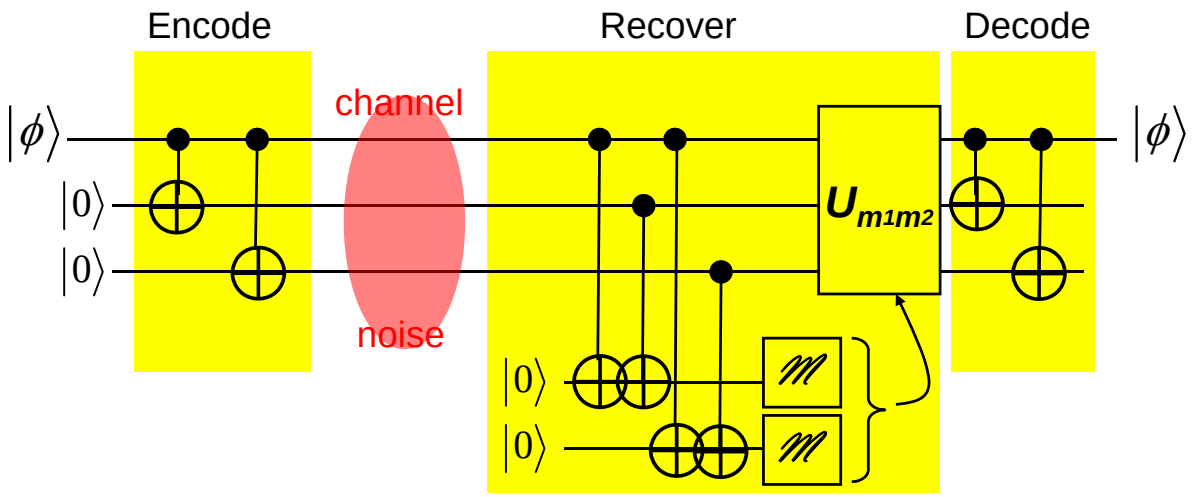
/u/divince/tex/tevtex/intro2000/divloss4

Ion Traps

- Couple lowest centre-of-mass modes to internal electronic states of N ions.



Quantum Error Correcting Code
Three Bit Code



Entanglement
EPR & Nonlocality

Alice ⇦ ☼ ⇨ Bob

$$\frac{1}{\sqrt{2}}\left(|1\rangle_A|0\rangle_B - |0\rangle_A|1\rangle_B\right) \neq |\psi\rangle_A \otimes |\phi\rangle_B$$

Local Hidden Variable → Bell's Inequality

Aspect's Experiment → Quantum Mechanics is nonlocal!

GHZ State: $\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B|0\rangle_C + |1\rangle_A|1\rangle_B|1\rangle_C\right)$

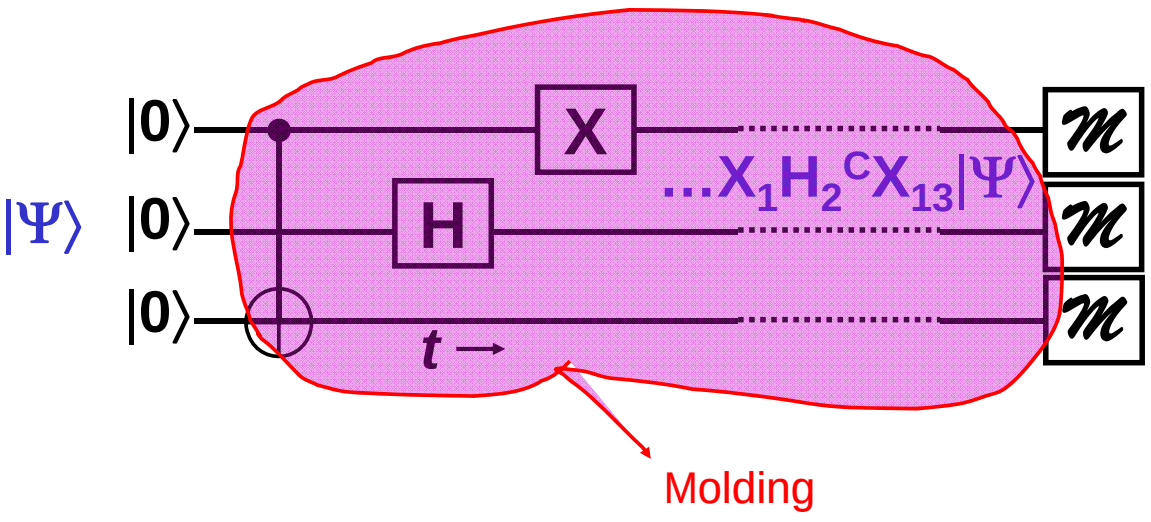
Charles Bennett's Hippie analogy

I don't know what I think.

You don't know what you think.

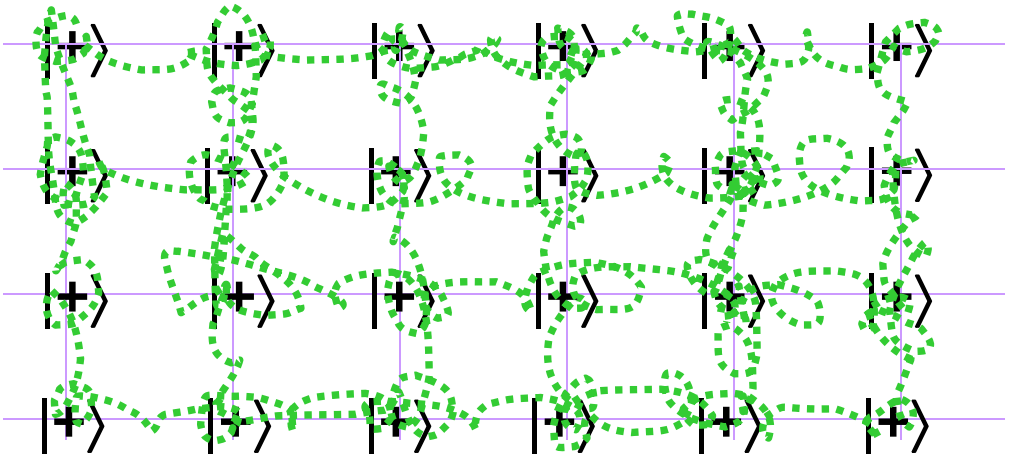
But we know what we think.

Molding a Quantum State



Sculpturing a Quantum State

- Cluster State Quantum Computing -



1. Initialize each qubit in $|+\rangle$ state.
2. Contolled-Phase between the neighboring qubits.
3. Single qubit manipulations and single qubit measurements only [Sculpturing].
   No two qubit operations!

Entanglement
EPR & Nonlocality

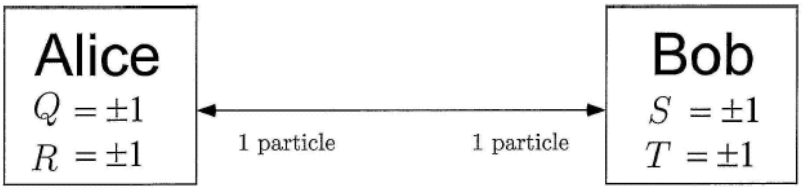
Alice ⇦ ☼ ⇨ **Bob**

$$\frac{1}{\sqrt{2}}\left(|1\rangle_A|0\rangle_B - |0\rangle_A|1\rangle_B\right) \neq |\psi\rangle_A \otimes |\phi\rangle_B$$

Local Hidden Variable → Bell's Inequality

Aspect's Experiment → Quantum Mechanics is nonlocal!

GHZ State: $\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B|0\rangle_C + |1\rangle_A|1\rangle_B|1\rangle_C\right)$



$$QS + RS + RT - QT = (Q + R)S + (R - Q)T$$

$$QS + RS + RT - QT = \pm 2$$

$$\begin{aligned}\mathbf{E}(QS + RS + RT - QT) &= \sum_{qrst} p(q,r,s,t)(qs + rs + rt - qt) \\ &\le \sum_{qrst} p(q,r,s,t) \times 2 \\ &= 2.\end{aligned}$$

$$\begin{aligned}\mathbf{E}(QS + RS + RT - QT) &= \sum_{qrst} p(q,r,s,t)qs + \sum_{qrst} p(q,r,s,t)rs \\ &\quad + \sum_{qrst} p(q,r,s,t)rt - \sum_{qrst} p(q,r,s,t)qt \\ &= \mathbf{E}(QS) + \mathbf{E}(RS) + \mathbf{E}(RT) - \mathbf{E}(QT).\end{aligned}$$

$$\mathbf{E}(QS) + \mathbf{E}(RS) + \mathbf{E}(RT) - \mathbf{E}(QT) \le 2.$$

Bell's inequality, CHSH inequality (Classical)

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

$$Q = Z_1 \qquad S = \frac{-Z_2 - X_2}{\sqrt{2}}$$

$$R = X_1 \qquad T = \frac{Z_2 - X_2}{\sqrt{2}}.$$

$$\langle QS\rangle = \frac{1}{\sqrt{2}};\ \langle RS\rangle = \frac{1}{\sqrt{2}};\ \langle RT\rangle = \frac{1}{\sqrt{2}};\ \langle QT\rangle = -\frac{1}{\sqrt{2}}.$$

$$\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2}.$$

Violation of inequality (Quantum)

Tripartite Qubit Entanglement

Z-basis: $|0\rangle$ with $+1$, $|1\rangle$ with -1

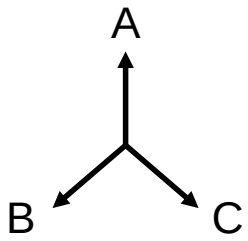
X-basis: $|a\rangle \approx |0\rangle + |1\rangle$ with $+1$, $|b\rangle \approx |0\rangle - |1\rangle$ with -1

$|0\rangle \approx |a\rangle + |b\rangle$, $|1\rangle \approx |a\rangle - |b\rangle$

Y-basis: $|c\rangle \approx |0\rangle + i|1\rangle$ with $+1$, $|d\rangle \approx |0\rangle - i|1\rangle$ with -1

$|0\rangle \approx |c\rangle + |d\rangle$, $|1\rangle \approx -i(|c\rangle - |b\rangle)$

Not expectation values



$$|GHZ\rangle = \frac{1}{\sqrt{2}}\{|000\rangle + |111\rangle\} \quad : \text{Z-basis}$$

$$\approx (a+b)(a+b)(a+b) + (a-b)(a-b)(a-b)$$

$$\approx aaa + abb + bab + bba \quad : xxx = +1$$

$$\approx (a+b)(c+d)(c+d) - (a-b)(c-d)(c-d)$$

$$\approx acd + adc + bcc + bdd \quad : xyy = -1$$

$xxx = +1$

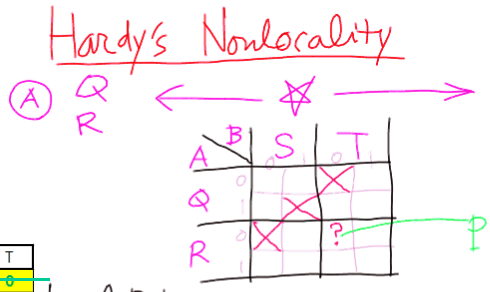
$xyy = -1$

$yxy = -1$

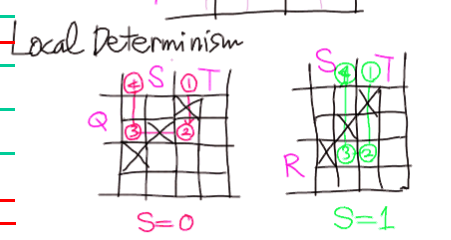
$yyx = -1$

$$(x^2y^2)_A (x^2y^2)_B (x^2y^2)_C = 1 \quad ?$$

Bipartite Qubit Entanglement



	Q	R	S	T
1	0	0	0	0
2	0	0	0	1
3	0	0	1	0
4	0	0	1	1
5	0	1	0	0
6	0	1	0	1
7	0	1	1	0
8	0	1	1	1
9	1	0	0	0
10	1	0	0	1
11	1	0	1	0
12	1	0	1	1
13	1	1	0	0
14	1	1	0	1
15	1	1	1	0
16	1	1	1	1



$$|\Psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + \underbrace{d}_{=0}|11\rangle \quad \text{with } |a|^2+|b|^2+|c|^2=1$$

$$\langle 00''|\Psi\rangle = 0 = a_B\langle 0''|0\rangle_B + b_B\langle 0''|1\rangle_B$$

$$\langle 0'0|\Psi\rangle = 0 = a_A\langle 0'|0\rangle_A + c_A\langle 0'|1\rangle_A$$

$$p = |\langle 0'0''|\Psi\rangle|^2 = |a|^2 \underbrace{|{}_A\langle 0'|0\rangle_A|^2}_{=p_A} \underbrace{|{}_B\langle 0''|0\rangle_B|^2}_{=p_B} = \frac{p_A p_B (1-p_A)(1-p_B)}{1-p_A p_B}$$

Maximize p !

$$\frac{\partial p}{\partial p_A} = \frac{\partial p}{\partial p_B} = 0 \Rightarrow 1-2p_A+p_A{}^2p_B = 1-2p_A+p_A{}^2p_B = 0$$

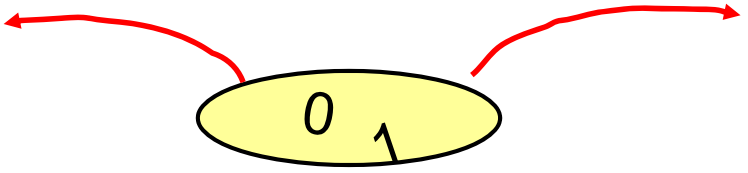
$$p_A = p_B = 1, \frac{-1\pm\sqrt{5}}{2} \Rightarrow p_A = p_B = \frac{\sqrt{5}-1}{2} = g: \text{ golden mean}$$

$$p = g^5 \approx 9\ \%$$

Entanglement

Quantum correlation

Alice x — Bob y



Classical physics: x and y are decided when picked up 0_A1_B or 1_A0_B

Quantum physics: x and y are decided when measured.

{0,1} basis → 0 or 1

{+,−} basis → + or −

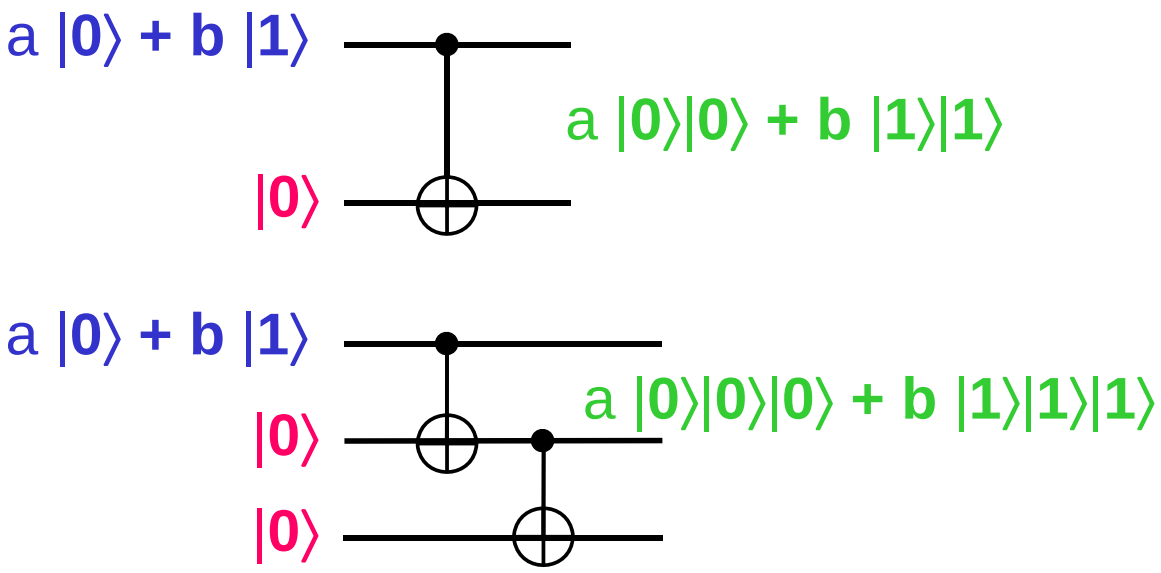
$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right)$$

$$= \frac{1}{\sqrt{2}}\left(|+\rangle_A|-\rangle_B - |-\rangle_A|+\rangle_B\right)$$

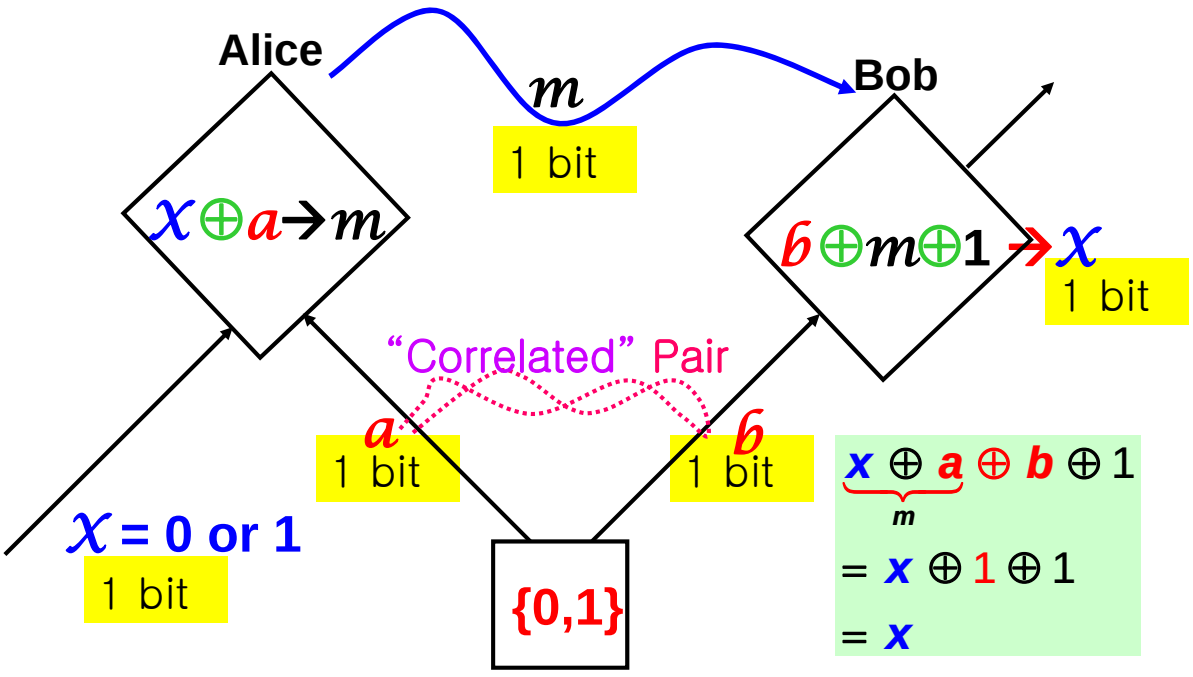
$$= \frac{1}{\sqrt{2}}\left(|0'\rangle_A|1'\rangle_B - |1'\rangle_A|0'\rangle_B\right)$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

Entanglement and Two-Qubit Gate

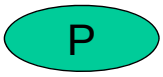


Classical Teleportation?

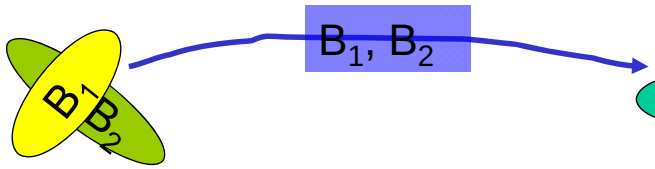


Quantum Teleportation

- **Transportation**
  - Continuous movement through space



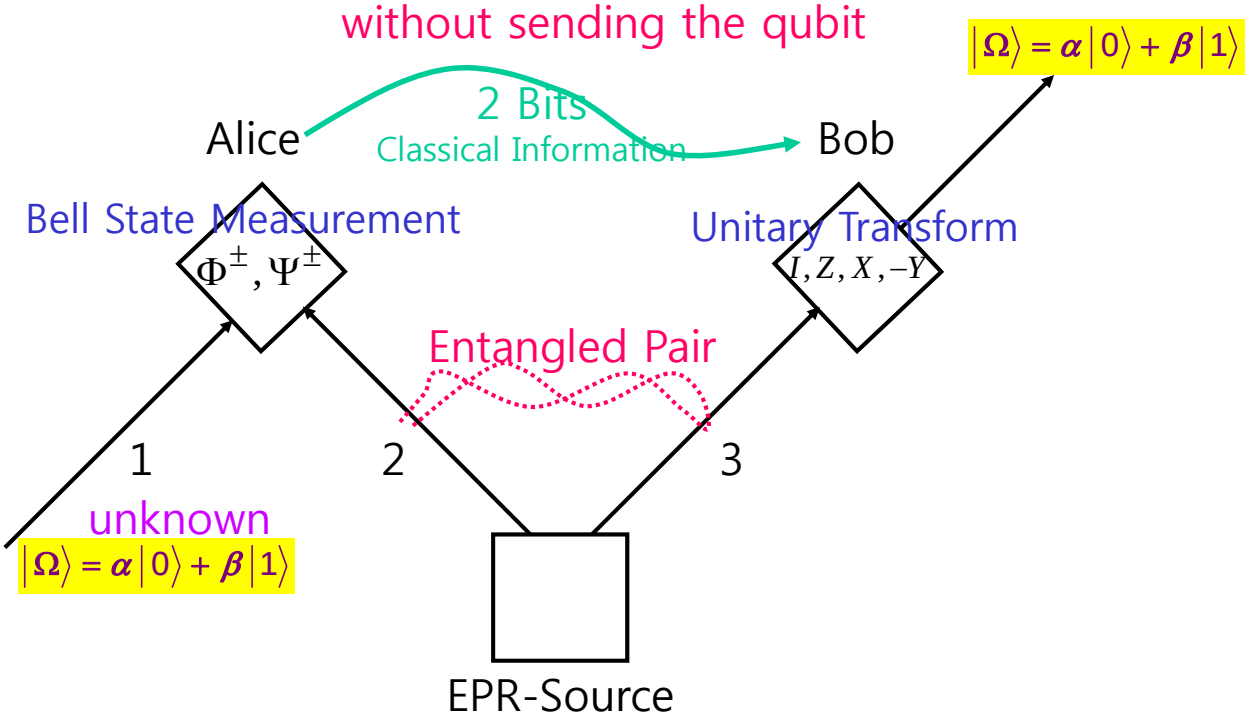
- **Quantum Teleportation**



Quantum Teleportation

Bennett

Transmit an unknown qubit
without sending the qubit



$$a|0\rangle_Q + b|1\rangle_Q \qquad \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right) \Rightarrow a|0\rangle_B + b|1\rangle_B$$

$|0\rangle_Q \to x$, $|1\rangle_Q \to y$; $|0\rangle_A \to x$, $|0\rangle_B \to x$, $|1\rangle_A \to y$, $|1\rangle_B \to y$

$$(ax+by)\left(xx+yy\right)/\sqrt{2} = (a\ b)\begin{pmatrix}x\\y\end{pmatrix}_Q (x\ y)_A \begin{pmatrix}x\\y\end{pmatrix}_B /\sqrt{2}$$

$X \cdot X = 1$, $\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}$

$$= (a\ b)\begin{pmatrix}xx & xy\\ yx & yy\end{pmatrix}_{QA}\begin{pmatrix}x\\y\end{pmatrix}_B/\sqrt{2} = (a\ b)\begin{pmatrix}xx & 0\\ 0 & yy\end{pmatrix}_{QA}\begin{pmatrix}x\\y\end{pmatrix}_B/\sqrt{2} + (a\ b)\begin{pmatrix}0 & xy\\ yx & 0\end{pmatrix}_{QA}\begin{pmatrix}x\\y\end{pmatrix}_B/\sqrt{2}$$

$$= \frac{1}{\sqrt{2}}(xx\ \ yy)_{QA}\begin{pmatrix}ax\\by\end{pmatrix}_B + \frac{1}{\sqrt{2}}(xy\ \ yx)_{QA}\begin{pmatrix}ay\\bx\end{pmatrix}_B$$

H on Q (HH) and H on A (HH)

$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}$, $H^2 = 1$

$$\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(xx\ \ yy)\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}ax\\by\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}\frac{xx+yy}{\sqrt{2}} & \frac{xx-yy}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}ax+by\\ax-by\end{pmatrix} = \frac{1}{\sqrt{2}}\left(\frac{xx+yy}{\sqrt{2}}\right)(ax+by) + \frac{1}{\sqrt{2}}\left(\frac{xx-yy}{\sqrt{2}}\right)(ax-by)$$

$$= \frac{1}{2}\left(\frac{xx+yy}{\sqrt{2}}\right)(ax+by) + \frac{1}{2}\left(\frac{xx-yy}{\sqrt{2}}\right)(ax-by) + \frac{1}{2}\frac{xy+yx}{\sqrt{2}}(ay+bx) + \frac{1}{2}\frac{xy-yx}{\sqrt{2}}(ay-bx)$$

$$= \frac{1}{2}\frac{|0\rangle|0\rangle+|1\rangle|1\rangle}{\sqrt{2}}(a|0\rangle+b|1\rangle) + \frac{1}{2}\frac{|0\rangle|0\rangle-|1\rangle|1\rangle}{\sqrt{2}}(a|0\rangle-b|1\rangle) + \frac{1}{2}\frac{|0\rangle|1\rangle+|1\rangle|0\rangle}{\sqrt{2}}(a|1\rangle+b|0\rangle) + \frac{1}{2}\frac{|0\rangle|1\rangle-|1\rangle|0\rangle}{\sqrt{2}}(a|1\rangle-b|0\rangle)$$

CNOT $|\ \rangle_Q|\ \rangle_A$

$$= \frac{1}{2}\frac{|0\rangle|0\rangle+|1\rangle|1\rangle}{\sqrt{2}}(a|0\rangle+b|1\rangle) + \frac{1}{2}\frac{|0\rangle|0\rangle-|1\rangle|1\rangle}{\sqrt{2}}(a|0\rangle-b|1\rangle) + \frac{1}{2}\frac{|0\rangle|1\rangle+|1\rangle|0\rangle}{\sqrt{2}}(a|1\rangle+b|0\rangle) + \frac{1}{2}\frac{|0\rangle|1\rangle-|1\rangle|0\rangle}{\sqrt{2}}(a|1\rangle-b|0\rangle)$$

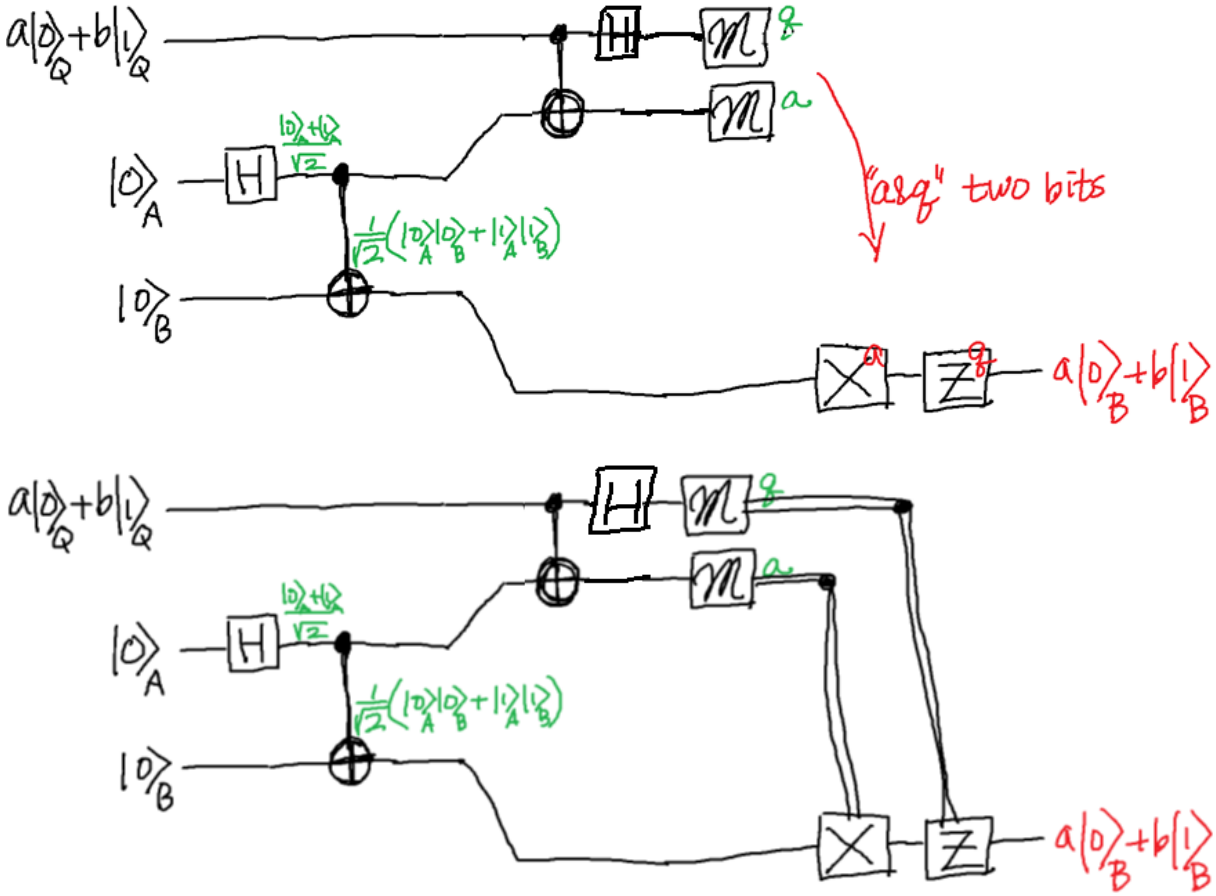
$$= \frac{1}{2}|+\rangle_Q|0\rangle_A(a|0\rangle_B+b|1\rangle_B) + \frac{1}{2}|-\rangle_Q|0\rangle_A(a|0\rangle_B-b|1\rangle_B) + \frac{1}{2}|+\rangle_Q|1\rangle_A(a|1\rangle_B+b|0\rangle_B) + \frac{1}{2}|-\rangle_Q|1\rangle_A(a|1\rangle_B-b|0\rangle_B)$$

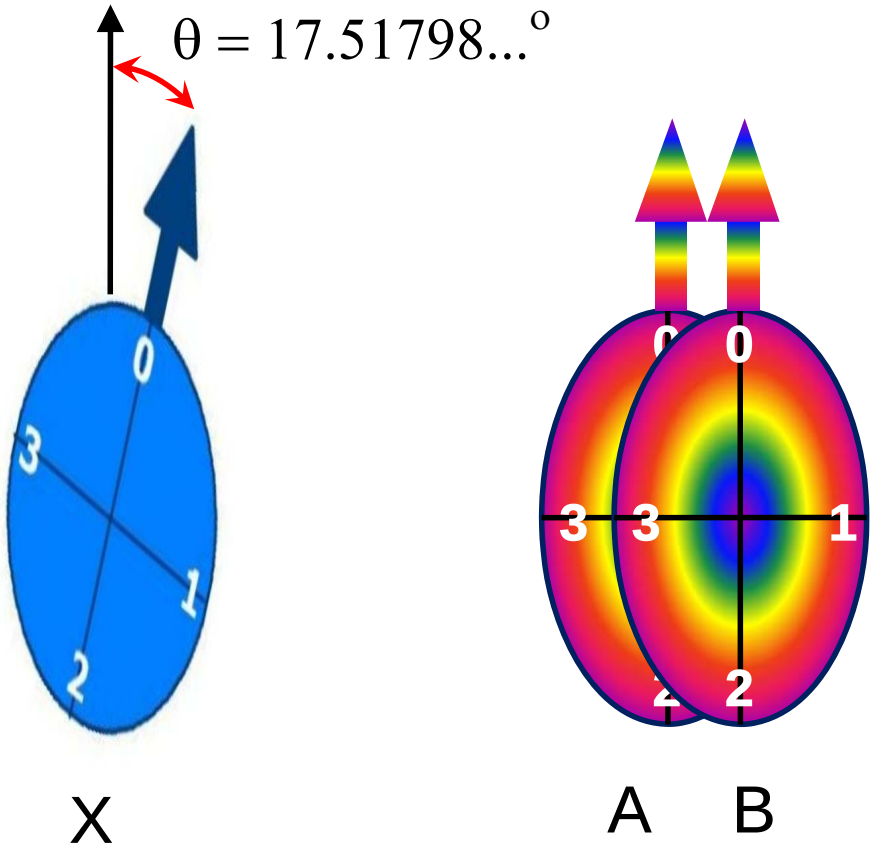
$H|\ \rangle_Q$

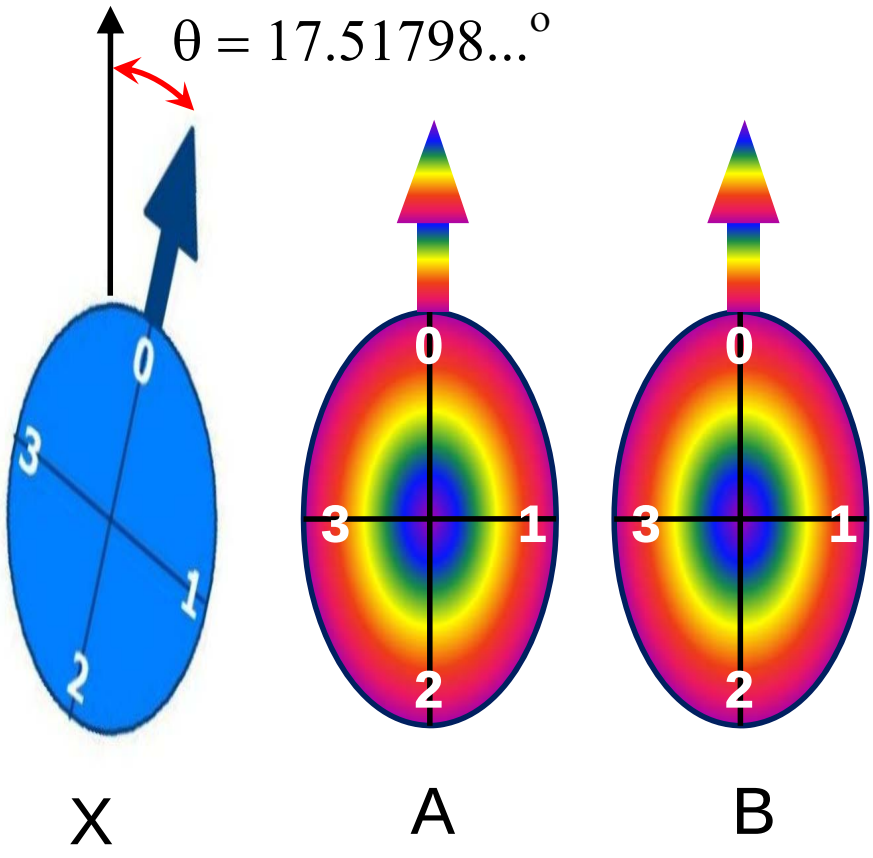
$$= \frac{1}{2}|0\rangle_Q|0\rangle_A(a|0\rangle_B+b|1\rangle_B) + \frac{1}{2}|1\rangle_Q|0\rangle_A(a|0\rangle_B-b|1\rangle_B) + \frac{1}{2}|0\rangle_Q|1\rangle_A(a|1\rangle_B+b|0\rangle_B) + \frac{1}{2}|1\rangle_Q|1\rangle_A(a|1\rangle_B-b|0\rangle_B)$$

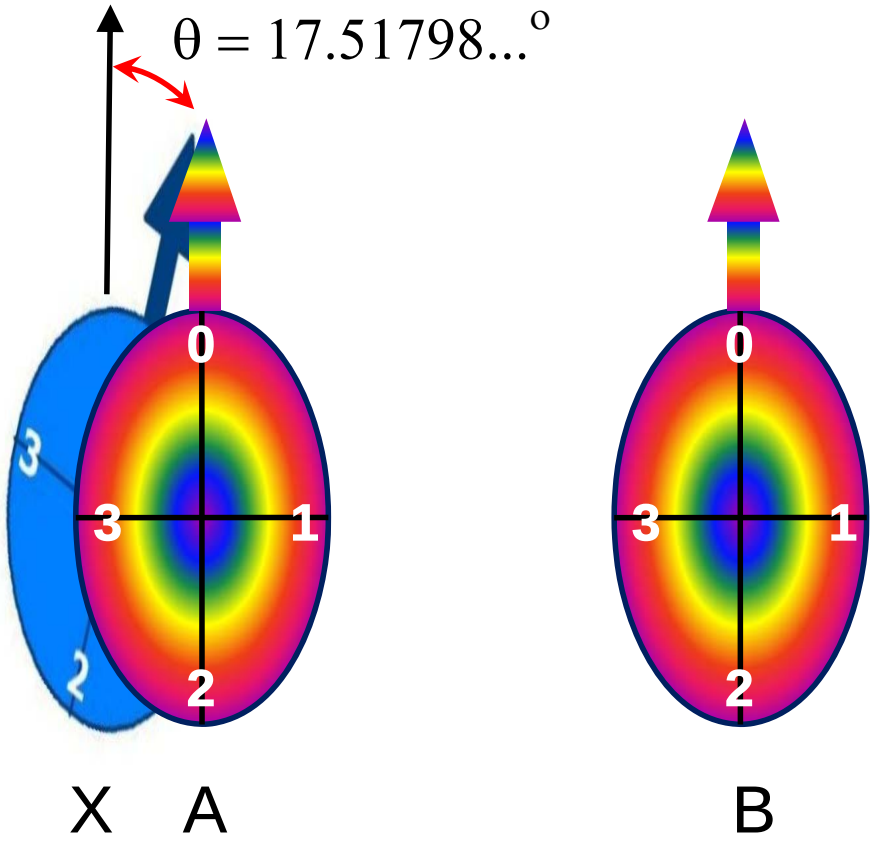
measure A → bit "a"
measure Q → bit "q"
⟹ send "a & q" to Bob. (two bits)

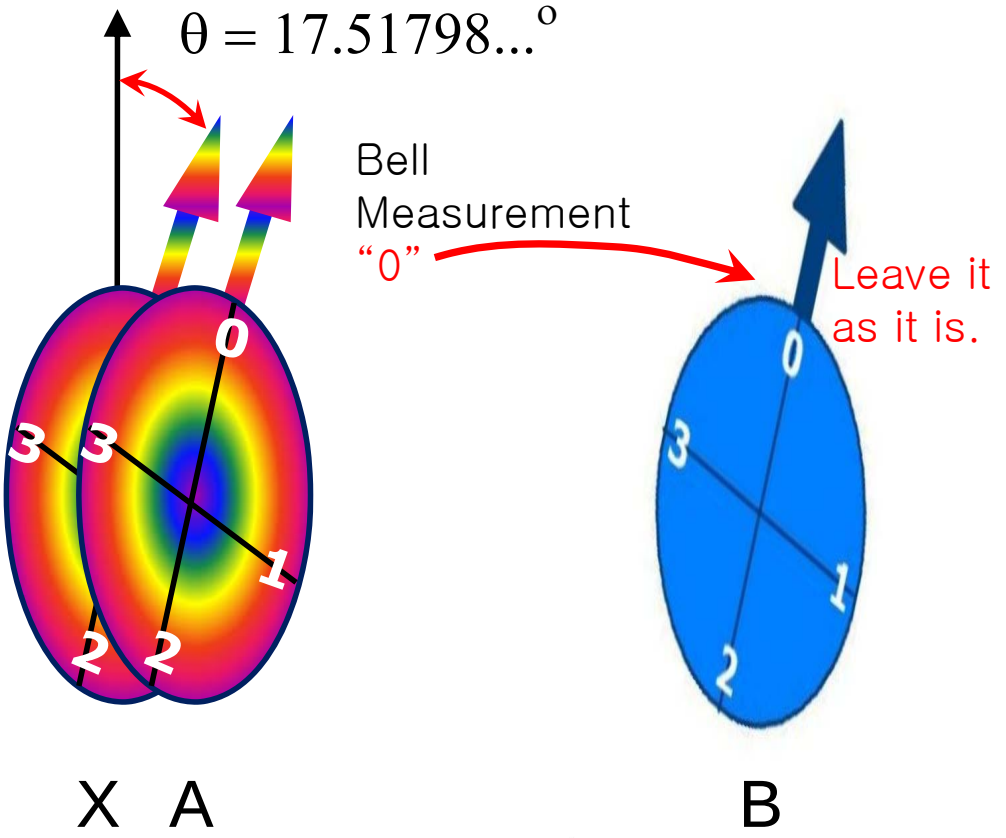
$$\Rightarrow Z_B^q X_B^a |\ \rangle_B = a|0\rangle_B + b|1\rangle_B$$

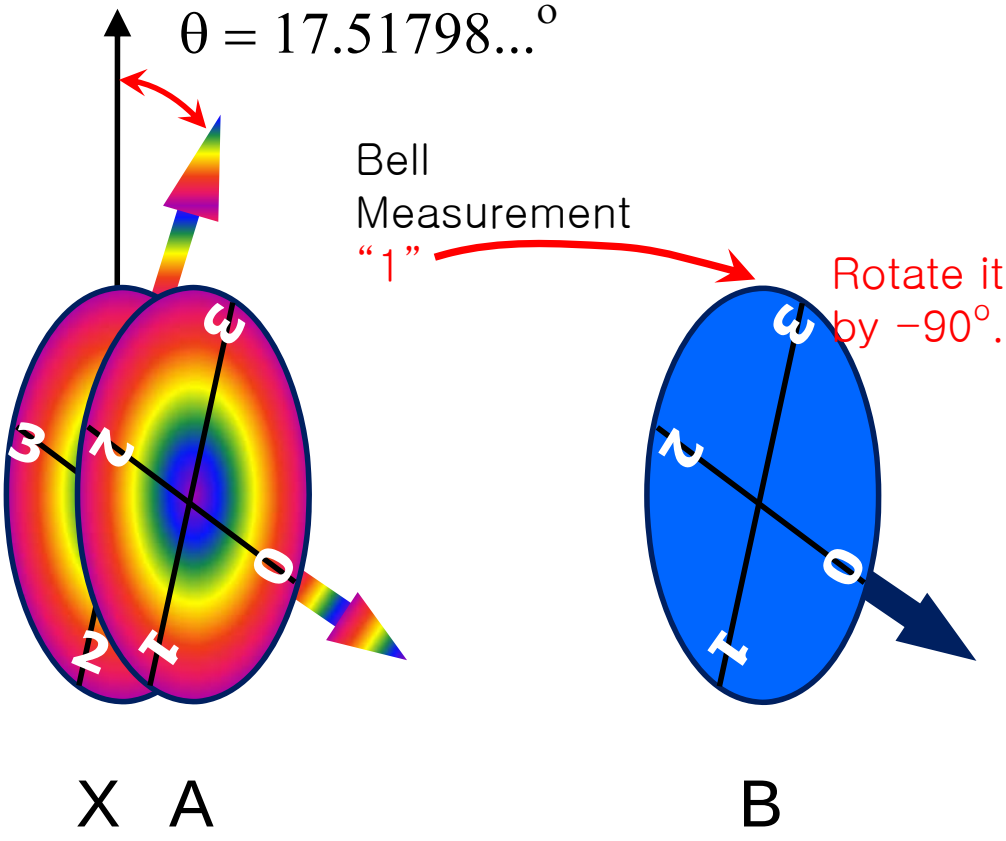

"asq" two bits

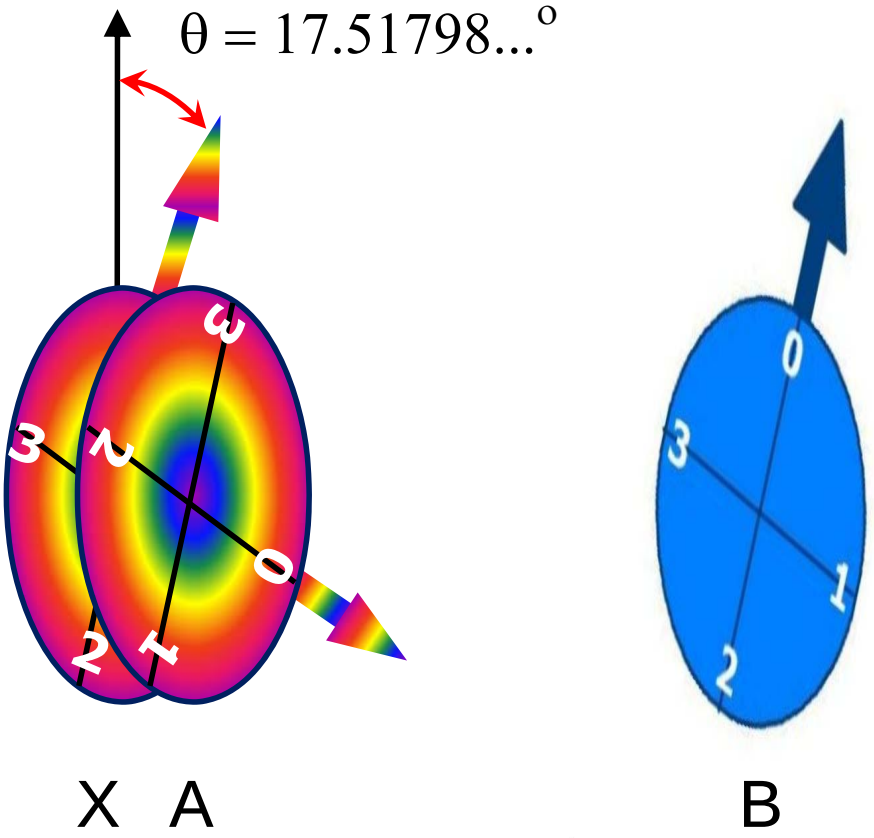

θ = 17.51798...°
0
3
1
2
0
3
3
1
2
X
A
B


θ = 17.51798...°
0
3
1
2
X
A
B


θ = 17.51798...°
0
3
1
2
X
A
B


θ = 17.51798...°
Bell
Measurement
"0"
Leave it
as it is.
0
3
3
1
2
2
0
3
1
2
X A
B


θ = 17.51798...°
Bell
Measurement
"1"
Rotate it
by −90°.
3
2
0
2
1
3
2
0
1
X A
B

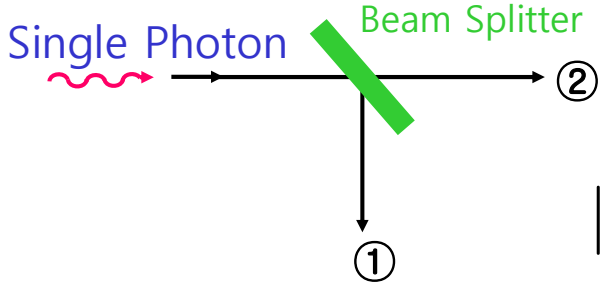


Single Particle Entanglement

$$H = -t\left(c_1^{+}c_2 + c_2^{+}c_1\right)$$

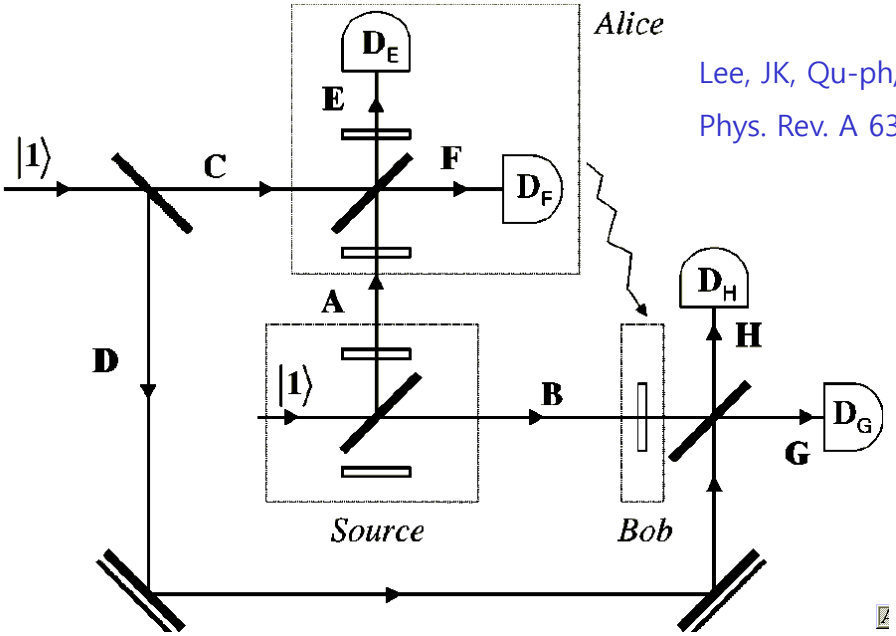
$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle + |2\rangle\right)$$

$$\text{or} \quad |\psi\rangle = \frac{1}{\sqrt{2}}\left(f_1 e_2 + e_1 f_2\right)$$



$$|\phi\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle|0\rangle + |0\rangle|1\rangle\right)$$

Quantum Teleportation
using Single Particle Entanglement



Lee, JK, Qu-ph/0007106;

Phys. Rev. A 63, 012305 (2001)

PRL88,070402 (2002) or QP/0204158

"Active" Teleportation of a Quantum Bit

S. Giacomini, F. Sciarrino, E. Lombardi and F. De Martini

VOLUME 88, NUMBER 7 PHYSICAL REVIEW LETTERS 18 FEBRUARY 2002

Teleportation of a Vacuum–One-Photon Qubit

Egilberto Lombardi,[1] Fabio Sciarrino,[1] Sandu Popescu,[2,3] and Francesco De Martini[1]

[1]Istituto Nazionale di Fisica della Materia, Dipartimento di Fisica, Università "La Sapienza," Roma, 00185 Italy

[2]H.H. Wills Physics Laboratory, University of Bristol, United Kingdom

[3]Hewlett-Packard Laboratories, Stoke Gifford, Bristol BS12-6QZ, United Kingdom

(Received 24 September 2001; published 30 January 2002)

We report the experimental realization of teleporting a one-particle entangled qubit. The qubit is physically implemented by a two-dimensional subspace of states of a mode of the electromagnetic field, specifically, the space spanned by the vacuum and the one-photon state. Our experiment follows the line suggested by Lee and Kim [Phys. Rev. A 63, 012305 (2000)] and Knill, Laflamme, and Milburn [Nature (London) 409, 46 (2001)]. An unprecedented large value of the teleportation "fidelity" has been attained: $F = (95.3 \pm 0.6)\%$.

articles

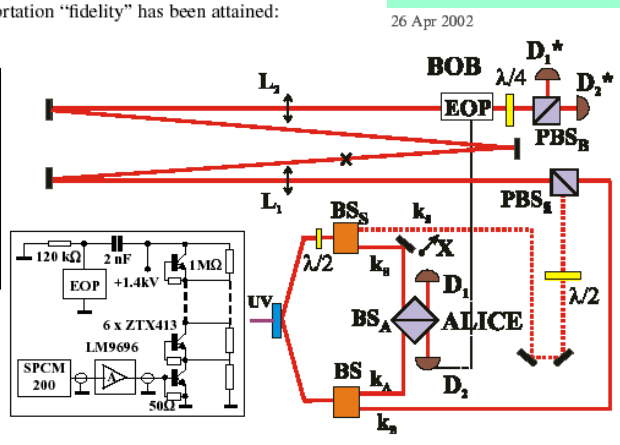
A scheme for efficient quantum computation with linear optics

E. Knill*, R. Laflamme† & G. J. Milburn†

* Los Alamos National Laboratory, MS B265, Los Alamos, New Mexico 87545, USA

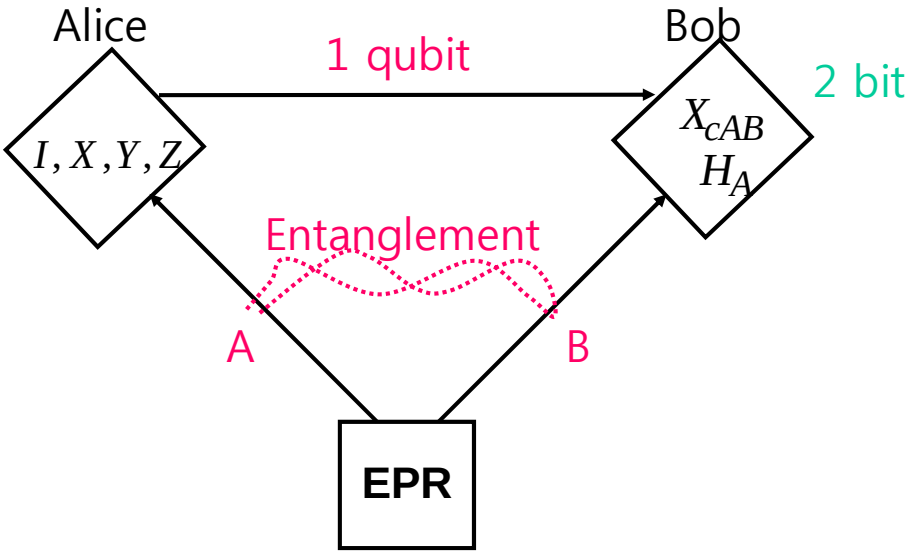
† Centre for Quantum Computer Technology, University of Queensland, St. Lucia, Australia

26 Apr 2002



Quantum Superdense Coding

Transmit two bits by sending one qubit



Quantum Superdense Coding

$$|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B \Rightarrow \begin{cases} I_A: |0\rangle|0\rangle + |1\rangle|1\rangle \\ X_A: |1\rangle|0\rangle + |0\rangle|1\rangle \\ Y_A: |1\rangle|0\rangle - |0\rangle|1\rangle \\ Z_A: |0\rangle|0\rangle - |1\rangle|1\rangle \end{cases} \Rightarrow X_{cAB}: \begin{cases} |0\rangle|0\rangle + |1\rangle|0\rangle = (|0\rangle + |1\rangle)|0\rangle \\ |1\rangle|1\rangle + |0\rangle|1\rangle = (|1\rangle + |0\rangle)|1\rangle \\ |1\rangle|1\rangle - |0\rangle|1\rangle = (|1\rangle - |0\rangle)|1\rangle \\ |0\rangle|0\rangle - |1\rangle|0\rangle = (|0\rangle - |1\rangle)|0\rangle \end{cases} \Rightarrow H_A: \begin{cases} |0\rangle|0\rangle \\ |0\rangle|1\rangle \\ |1\rangle|1\rangle \\ |1\rangle|0\rangle \end{cases}$$

Alice's manipulation

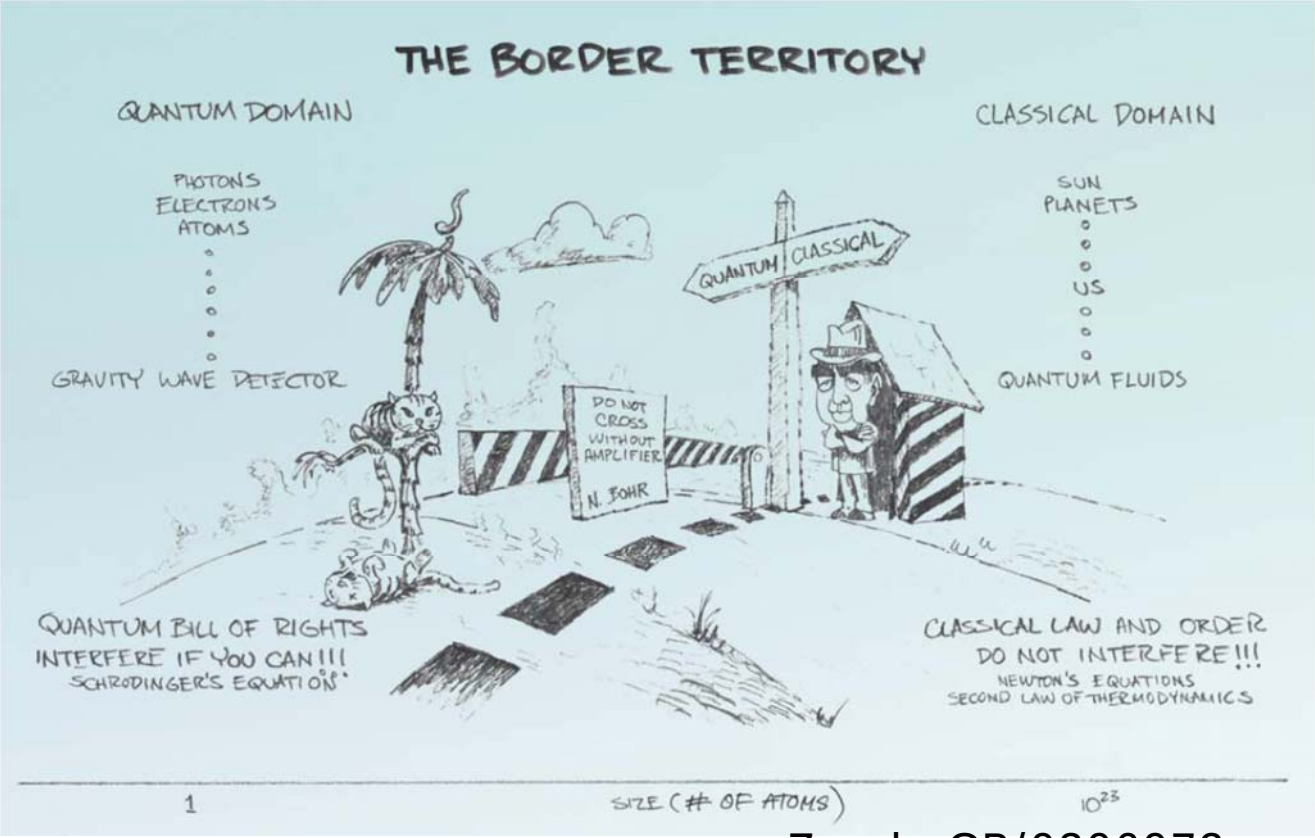
Bob's manipulation

Alice sends the qubit to Bob

1 qubit

4 states differentiated

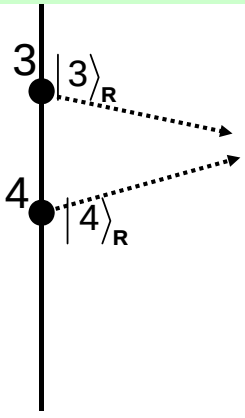
2 bit



Zurek, QP/0306072

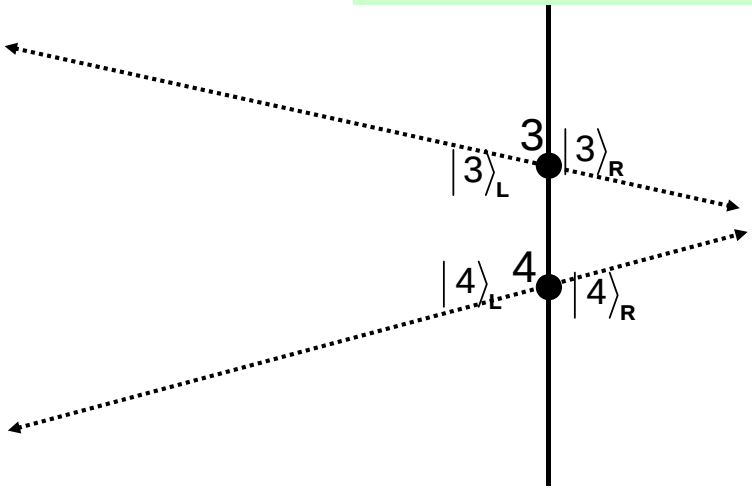
$$|\varphi\rangle = \frac{1}{\sqrt{2}}\left(|3\rangle_R + |4\rangle_R\right)$$

$$\rho_{LR} = |\varphi\rangle\langle\varphi| = \begin{matrix} |3\rangle \\ |4\rangle \end{matrix} \overbrace{\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}}^{\langle 3| \quad \langle 4|}$$



$$|\varphi\rangle = \frac{1}{\sqrt{2}}\left(|3\rangle_L |3\rangle_R + |4\rangle_L |4\rangle_R\right)$$

$$\rho_{LR} = |\varphi\rangle\langle\varphi|$$

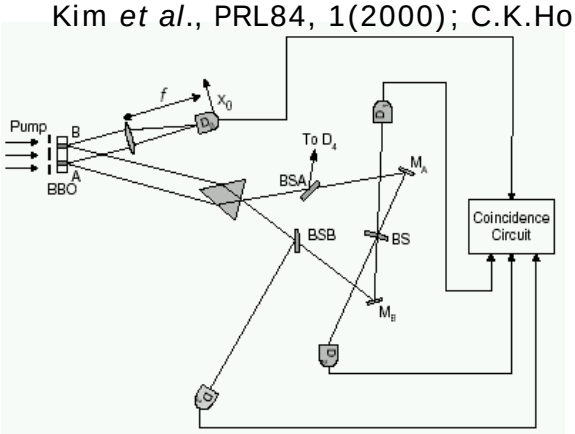


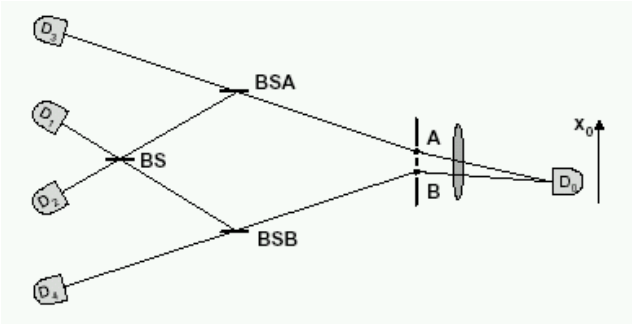
C K Hong and T Noh (1998)
Y-H Kim and Y Shi (2000)

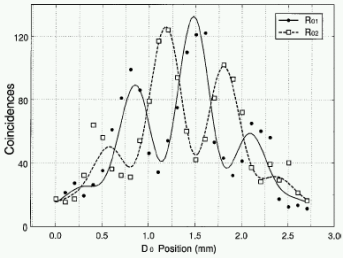
Delayed Choice Quantum Erasure

REVISITED

Kim *et al*., PRL84, 1(2000); C.K.Hong and T.G.Noh, JOSA B15, 1192(1998)







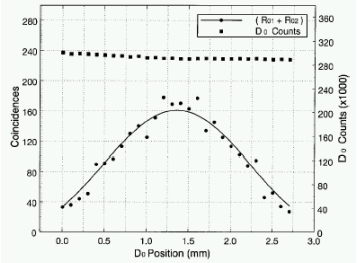


FIG. 4. $R_{01} + R_{02}$ is shown. The solid line is a fit to the sinc function given in Eq. (6). The single counting rate of D_0 is constant over the scanning range.

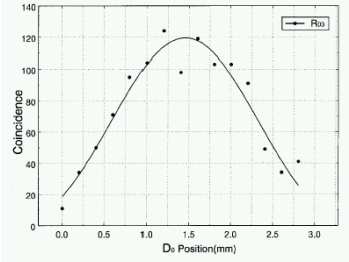
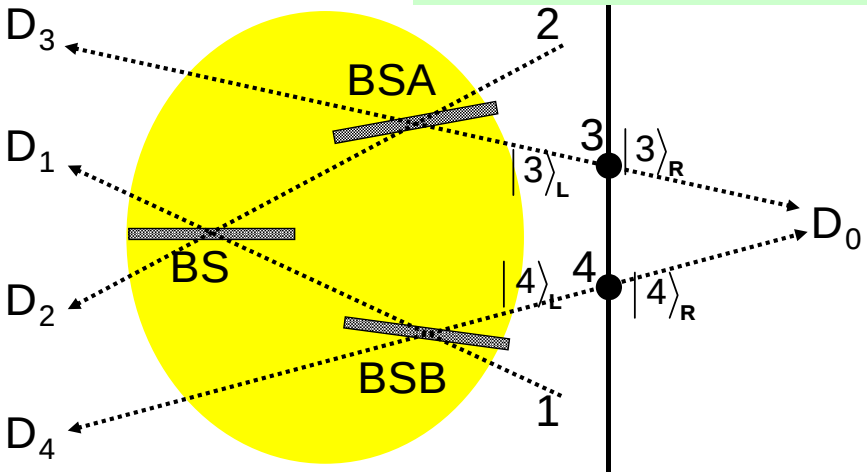


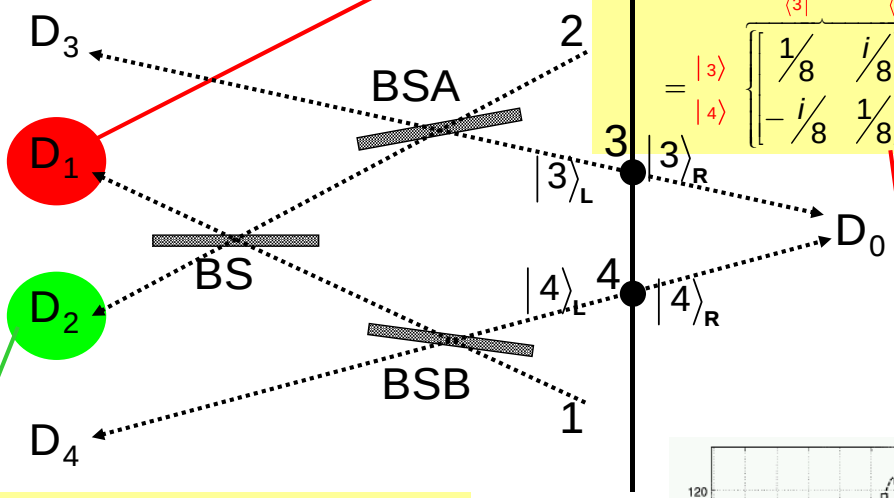
FIG. 5. R_{03} is shown. Absence of interference is clearly demonstrated. The solid line is a fit to the sinc function given in Eq. (6).

$$\rho'_{LR} = U_L |\varphi\rangle\langle\varphi| U_L^+ = \frac{1}{2}\left\{\left(-\frac{|1\rangle_L}{2} + i\frac{|2\rangle_L}{2} + \frac{|3\rangle_L}{\sqrt{2}}\right)|3\rangle_R + \left(i\frac{|1\rangle_L}{2} - \frac{|2\rangle_L}{2} + \frac{|4\rangle_L}{\sqrt{2}}\right)|4\rangle_R\right\}\{h.c.\}$$

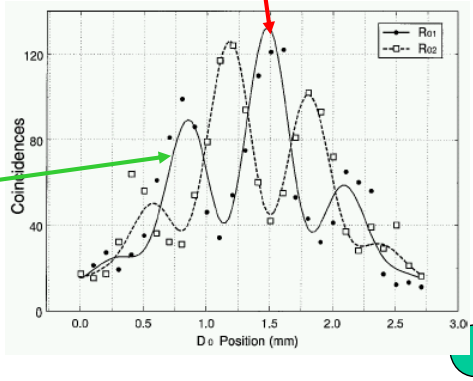


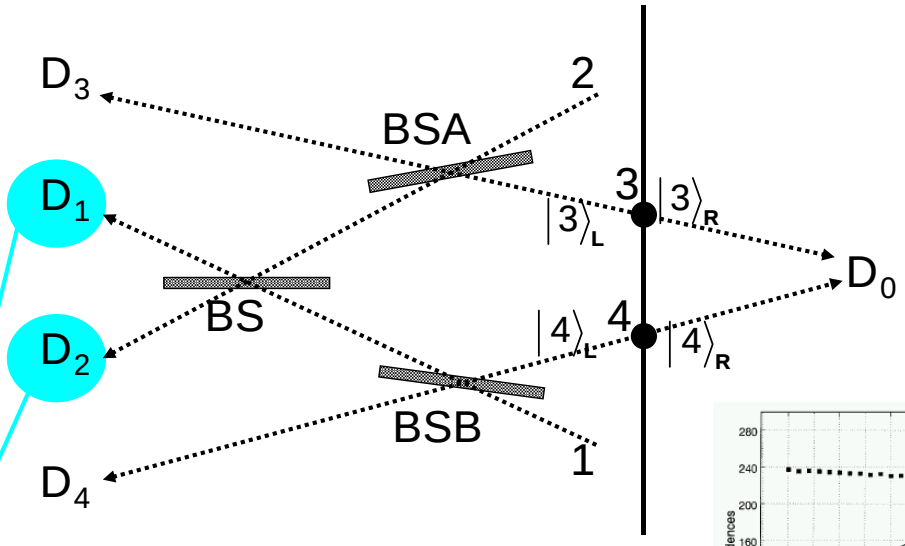
$$U_L = \begin{bmatrix} 1/2 & i/2 & -1/2 & i/2 \\ i/2 & 1/2 & i/2 & -1/2 \\ 0 & i/\sqrt{2} & 1/\sqrt{2} & 0 \\ i/\sqrt{2} & 0 & 0 & 1/\sqrt{2} \end{bmatrix}$$

$$\rho'_{R|D_1} = {}_L\langle 1|U_L|\varphi\rangle\langle\varphi|U_L^+|1\rangle_L$$
$$= \frac{1}{8}\{-|3\rangle_R + i|4\rangle_R\}\{-{}_R\langle 3| - i\,{}_R\langle 4|\}$$
$$= \begin{matrix} \\ |3\rangle \\ |4\rangle \end{matrix} \overbrace{\begin{bmatrix} 1/8 & i/8 \\ -i/8 & 1/8 \end{bmatrix}}^{\langle 3| \quad \langle 4|}$$



$$\rho'_{R|D_2} = {}_L\langle 2|U_L|\varphi\rangle\langle\varphi|U_L^+|2\rangle_L$$
$$= \frac{1}{8}\{i|3\rangle_R - |4\rangle_R\}\{-i\,{}_R\langle 3| - {}_R\langle 4|\}$$
$$= \begin{matrix} \\ |3\rangle \\ |4\rangle \end{matrix} \overbrace{\begin{bmatrix} 1/8 & -i/8 \\ i/8 & 1/8 \end{bmatrix}}^{\langle 3| \quad \langle 4|}$$





$$\rho'_{R|(D_1+D_2)} = \begin{bmatrix} 1/8 & i/8 \\ -i/8 & 1/8 \end{bmatrix} + \begin{bmatrix} 1/8 & -i/8 \\ i/8 & 1/8 \end{bmatrix} = \begin{bmatrix} 1/4 & 0 \\ 0 & 1/4 \end{bmatrix}$$

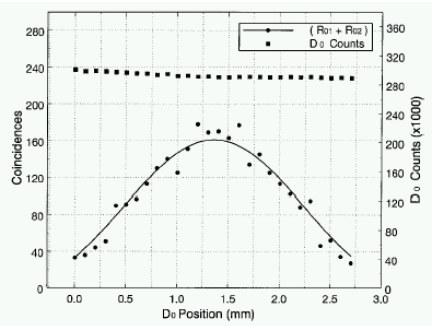


FIG. 4. $R_{01} + R_{02}$ is shown. The solid line is a fit to the sinc function given in Eq. (6). The single counting rate of D_0 is constant over the scanning range.

$$\rho'_{R|D_3} = {}_L\langle 3|U_L|\varphi\rangle\langle\varphi|U_L^+|3\rangle_L = \frac{1}{4}|3\rangle_R\,{}_R\langle 3| = \begin{bmatrix} 1/4 & 0 \\ 0 & 0 \end{bmatrix}$$

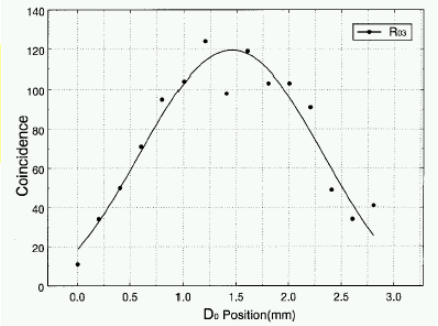
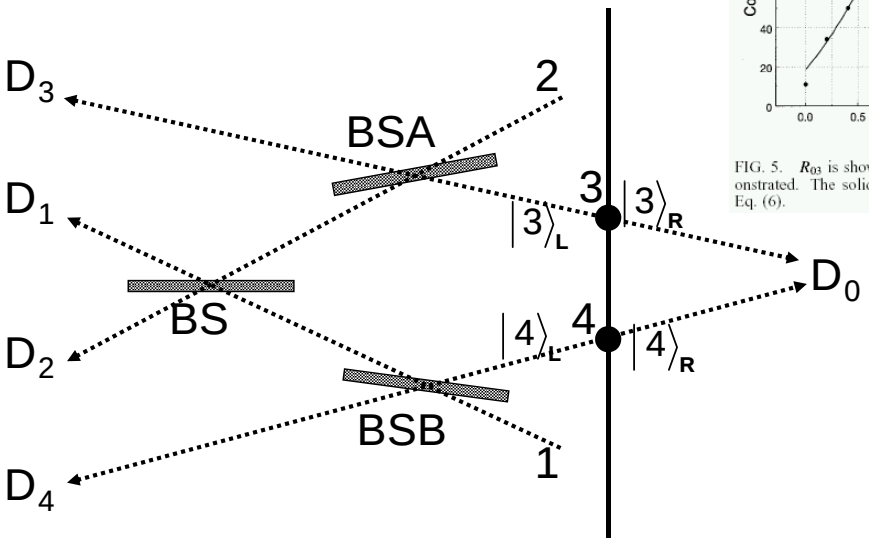


FIG. 5. R_{03} is shown. Absence of interference is clearly demonstrated. The solid line is a fit to the sinc function given in Eq. (6).



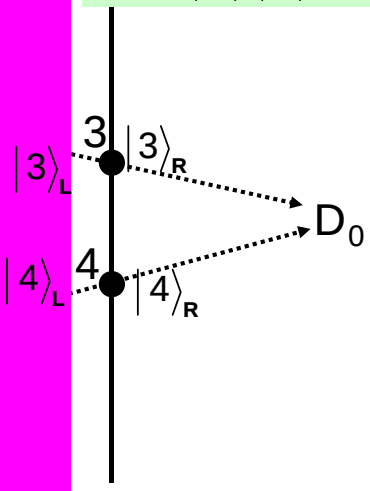
$$\rho'_{R|D_4} = {}_L\langle 4|U_L|\varphi\rangle\langle\varphi|U_L^+|4\rangle_L = \frac{1}{4}|4\rangle_R\,{}_R\langle 4| = \begin{bmatrix} 0 & 0 \\ 0 & 1/4 \end{bmatrix}$$

Environment

Decoherence

$$|\varphi\rangle = \frac{1}{\sqrt{2}}\left(|3\rangle_L |3\rangle_R + |4\rangle_L |4\rangle_R\right)$$

$$\rho_{LR} = |\varphi\rangle\langle\varphi|$$



$$\rho_R = \mathrm{tr}_L \rho_{LR} = \frac{1}{2}\left\{|3\rangle_{R\ R}\langle 3| + |4\rangle_{R\ R}\langle 4|\right\} = \frac{1}{2}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

$$\rho'_{R|(D_1+D_2+D_3+D_4)} = \begin{bmatrix}1/4 & 0\\ 0 & 1/4\end{bmatrix} + \begin{bmatrix}1/4 & 0\\ 0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0\\ 0 & 1/4\end{bmatrix} = \begin{bmatrix}1/2 & 0\\ 0 & 1/2\end{bmatrix}$$

Cryptography and QIP

-병 주고 약 주고-

Giving disease,
Giving medicine.

Out with the old,
In with the new.

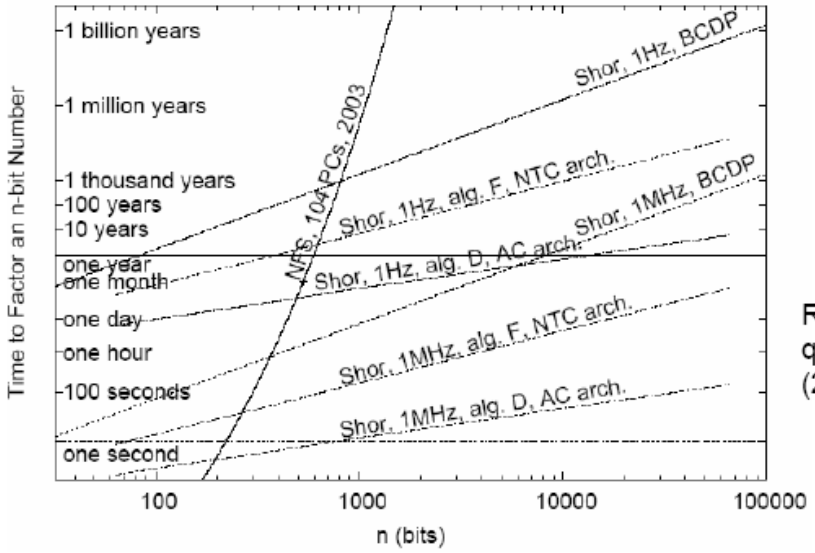
- **Public Key Cryptosystem (Asymmetric)**
  - **Computationally Secure**
  - **Based on unproven mathematical conjectures**
  - **Cursed by Quantum Computation**
- **One-Time Pad (Symmetric)**
  - **Unconditionally Secure**
  - **Impractical**
  - **Saved by Quantum Cryptography**

The Factoring Problem

Best known classical algorithm: Number Field Sieve

RSA-640 (193 digits) factored with 30 2.2GHz-Opteron CPU years (5 calendar months) http://www.rsa.com/rsalabs/node.asp?id=2093

Implementation architecture makes a big difference!!



R. Van Meter et al., quant-ph/0507023 (2005)

"*Quantum Key Distribution* is a major paradigm shift in the development of cryptography.

Conventional and quantum cryptography are a powerful combination in making a secure communications a reality."

-Burt Kaliski, Chief Scientist, **RSA** Laboratories

[Symmetric]

One-Time pad


Alice

Bob 

Tell me the password.

Pass word + key =

4672856


Eve

4672856

4672856 – key
= pass word

[Symmetric]

One-Time Pad

Vernam

- **Alice**

$$\begin{array}{rl} & M = 01100110001 \\ \oplus & K = 01010100101 \quad \text{(random)} \\ \hline & E = 00110010100 \end{array}$$

- **Bob**

$$\begin{array}{rl} & E = 00110010100 \\ \oplus & K = 01010100101 \quad \text{(random)} \\ \hline & M = 01100110001 \end{array}$$

- **Unconditionally Secure**
- **Impractical: Generation and Distribution**

Encoding

M⊕K: 0⊕0=0, 0⊕1=1, 1⊕0=1, 1⊕1=0

KEY

```
11011001011011001010101010101010010101010
01010101001010100111001000101001010101010
10010101001010101010010101101010100101010
01010100101001010101001011010010100010010
10010101001010101010010101101010011001111
```

Cypher Text

```
11011101011000111000100001010010010101010
01010001001110101101000010101001010101010
10010001001110101000001111001001010010101010
01010000101101011100011001010010100010010
10010010111001011001110101010010011001111
```

KEY

```
11011001011001000100100100000010010101010
01010010010010101001100010010100101010101010
10010010010010101000001010000010100101010
01010001010010101010001001010010100010010
10010000010000100100101010000010011001111
```

[Symmetric]

Why is it called One-Time?

- E1 = M1 ⊕ K
- E2 = M2 ⊕ K
- E1 ⊕ E2

  = (M1 ⊕ K) ⊕ (M2 ⊕ K)

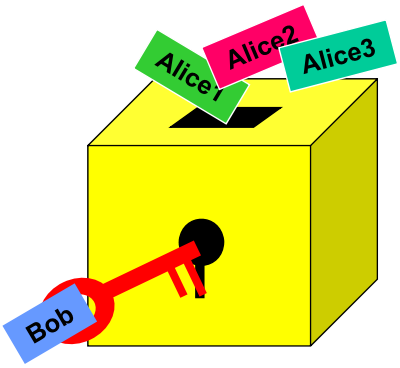
  = M1 ⊕ M2 ⊕ (K ⊕ K)

  = M1 ⊕ M2 ⊕ (0)

  = M1 ⊕ M2

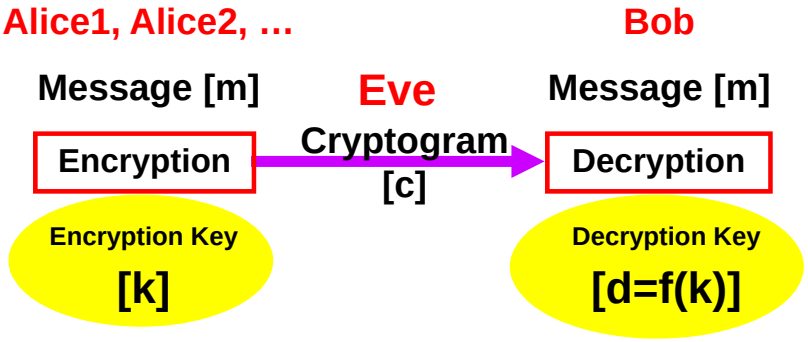
[Asymmetric]

Public Key Cryptosystem



Diffie, Hellman

RSA : Rivest, Shamir, Adleman



- Computationally Secure
- Could be broken,
  especially by Quantum Computers

[Asymmetric]

RSA Cryptosystem

- Message ➔ M
- n = p q , e d = 1 mod (p-1)(q-1)
  - n, e : Public Key (Encryption)
  - n, d : Secret Key (Decryption)
- Alice : $E = M^e \bmod n$
- Bob : $M = E^d \bmod n$
- M ➔ Message

RSA Example

- **Bob's Keys**
  - p = 11, q = 13, n = p q = 143
  - d = 103, e = 7
  - d e mod (p-1)(q-1) = 103 x 7 mod 120 = 1
- **Alice's Message:**
  - M = 9
  - $E = M^e \bmod n = 9^7 \bmod 143 = 48$
- **Bob**
  - $M = E^d \bmod n = 48^{103} \bmod 143 = 9$

How Hard is Factoring?

- **Almost exponentially complex with the number of digits, L**
- **RSA129 (1977)**
  - Factored 17 years later using 1,600 computers
- **2,000 Digit Number** Vazirani

  Impossible to factor even
  - With as many digital computers as the number of particles in the Universe (10^{80})
  - In as long time as the age of the universe (10^{18} sec)

PRIMES is in P

Manindra Agrawal, Neeraj Kayal and Nitin Saxena*

Department of Computer Science & Engineering
Indian Institute of Technology Kanpur
Kanpur-208016, INDIA

August 6, 2002

We present a deterministic polynomial-time algorithm that determines whether an input number n is prime or composite.

"The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length... Further, the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated."

- Karl Friedrich Gauss, *Disquisitiones Arithmeticae*, 1801 (translation from [Kmu98])

No Cloning Theorem

An Unknown Quantum State Cannot Be Cloned.

Zurek, Wootters
Diks

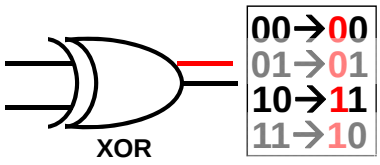
<Proof>

$$U\left(|\alpha\rangle|0\rangle\right)=|\alpha\rangle|\alpha\rangle$$

$$U\left(|\beta\rangle|0\rangle\right)=|\beta\rangle|\beta\rangle \qquad |\alpha\rangle \neq |\beta\rangle$$

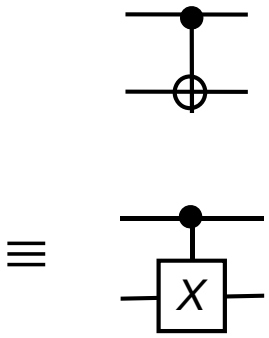
$$\text{Let } |\gamma\rangle=\frac{1}{\sqrt{2}}\left(|\alpha\rangle+|\beta\rangle\right).$$

$$\text{Then } \quad U\left(|\gamma\rangle|0\rangle\right)=\frac{1}{\sqrt{2}}\left(|\alpha\rangle|\alpha\rangle+|\beta\rangle|\beta\rangle\right)\neq|\gamma\rangle|\gamma\rangle$$



$$X_{AB} = |0\rangle_{AA}\langle 0| \otimes I_B + |1\rangle_{AA}\langle 1| \otimes X_B$$

Controlled-NOT

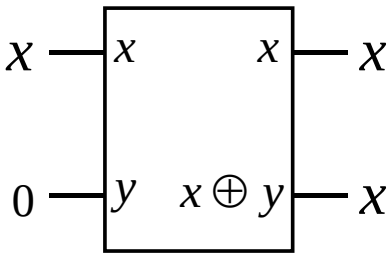


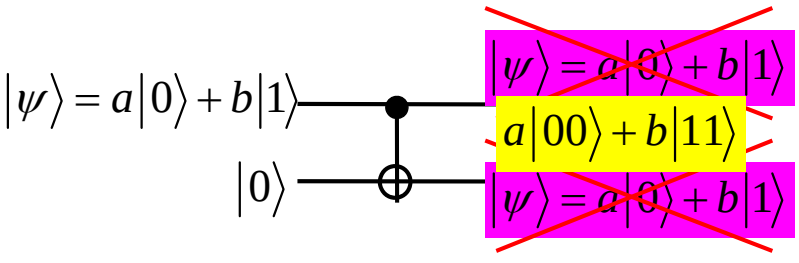
$$= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}_A \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}_B + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}_A \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}_B$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}_{AB} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{AB}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{AB}$$

Qubit Copying Circuit?





If an unknow quantum state Can be cloned …

- **Quantum States can be measured as accurately as possible ???**

  $|\psi\rangle \Rightarrow |\psi\rangle , |\psi\rangle , |\psi\rangle , |\psi\rangle$ …

  measure, measure, …

- **Commnunication Faster Than Light?**

  $|\psi\rangle = |0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B$ for "0"

  $= |+\rangle_A |-\rangle_B + |-\rangle_A |+\rangle_B$ for "1"

Communication Faster Than Light

when unknown quantum state can be copied.

- Alice wants to send Bob "1."
  Alice mesures her qubit in {|+**>,|->}.**
- Alice's state will become |+> or |->.
- Bob's state will become |-> or |+>.
  Let's assume it is |+>.
- Bob makes many copies of this.
  He measures them in {|+>, |->}, and gets 100% |+>.
  He measures them in {|0>, |1>}, and gets 50% |0> and 50% |1>.
  Thus Bob can conclude that Alice measured her state in {|+>, |->}.

Mysterious Connection Between QM & Relativity

- Weinberg: Can QM be nonlinear?
- Experiments: Not so positive result.
- Polchinski, Gisin:
  If QM is nonlinear,
  communication faster than light is possible.

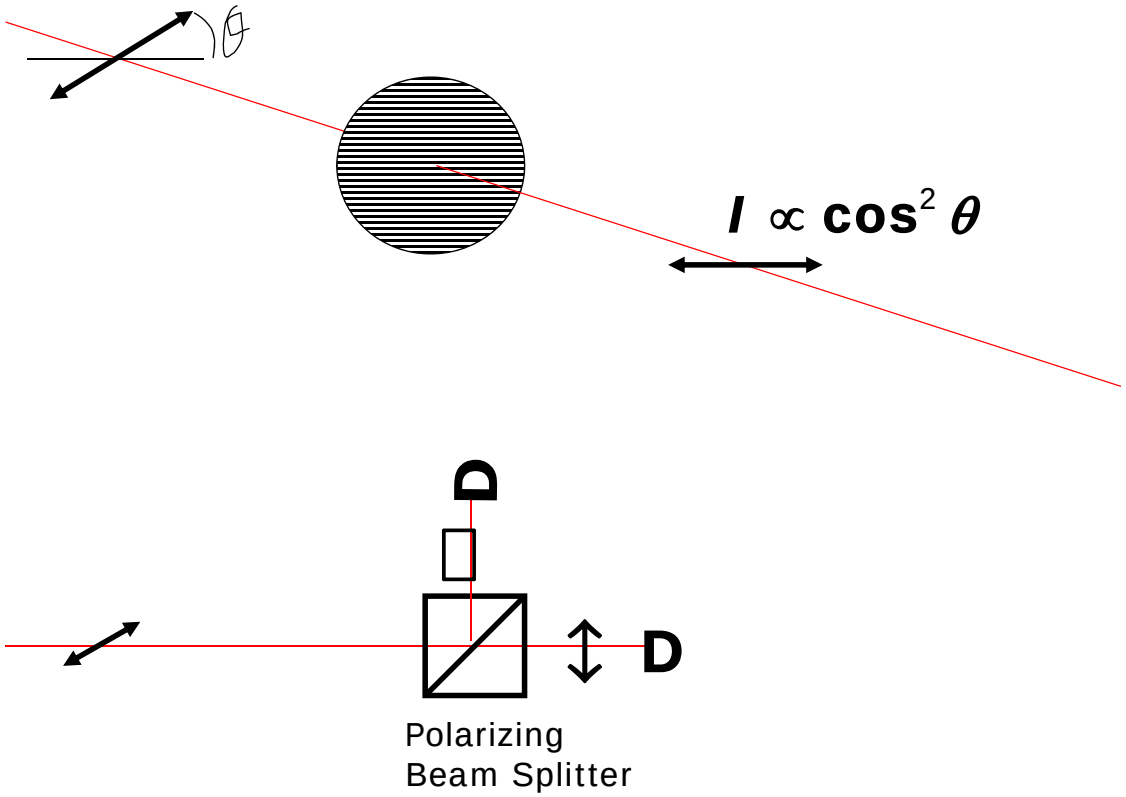
Irreversability of Quantum Measurement

"道可道 非常道 名可名 非常名" –老子–

$$|\psi\rangle = a|0\rangle + b|1\rangle = c|0'\rangle + d|1'\rangle$$

Measure in $\{|0\rangle, |1\rangle\}$ ➔ $|0\rangle$ or $|1\rangle$

Measure in $\{|0'\rangle, |1'\rangle\}$ ➔ $|0'\rangle$ or $|1'\rangle$

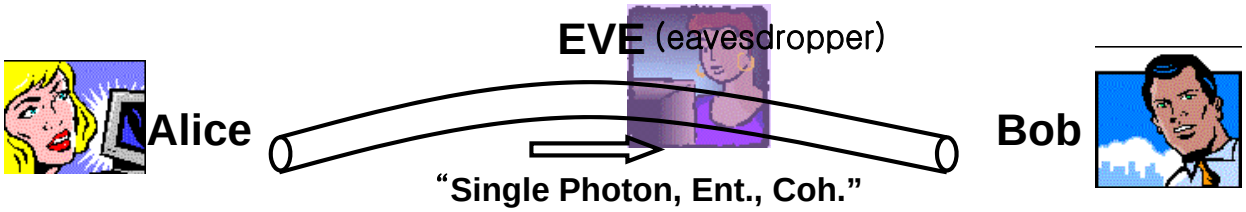


Quantum Cryptography

Quantum Key Distribution

BB84, B92, E91

No Cloning & Irreversability of Quantum Measurement



1. **Interconvertibility between stationary and flying qubits.**
2. **Faithful transmission of flying qubits.**

DiVincenzo, Qu-Ph/0002077

BB84: 4 Polarizations

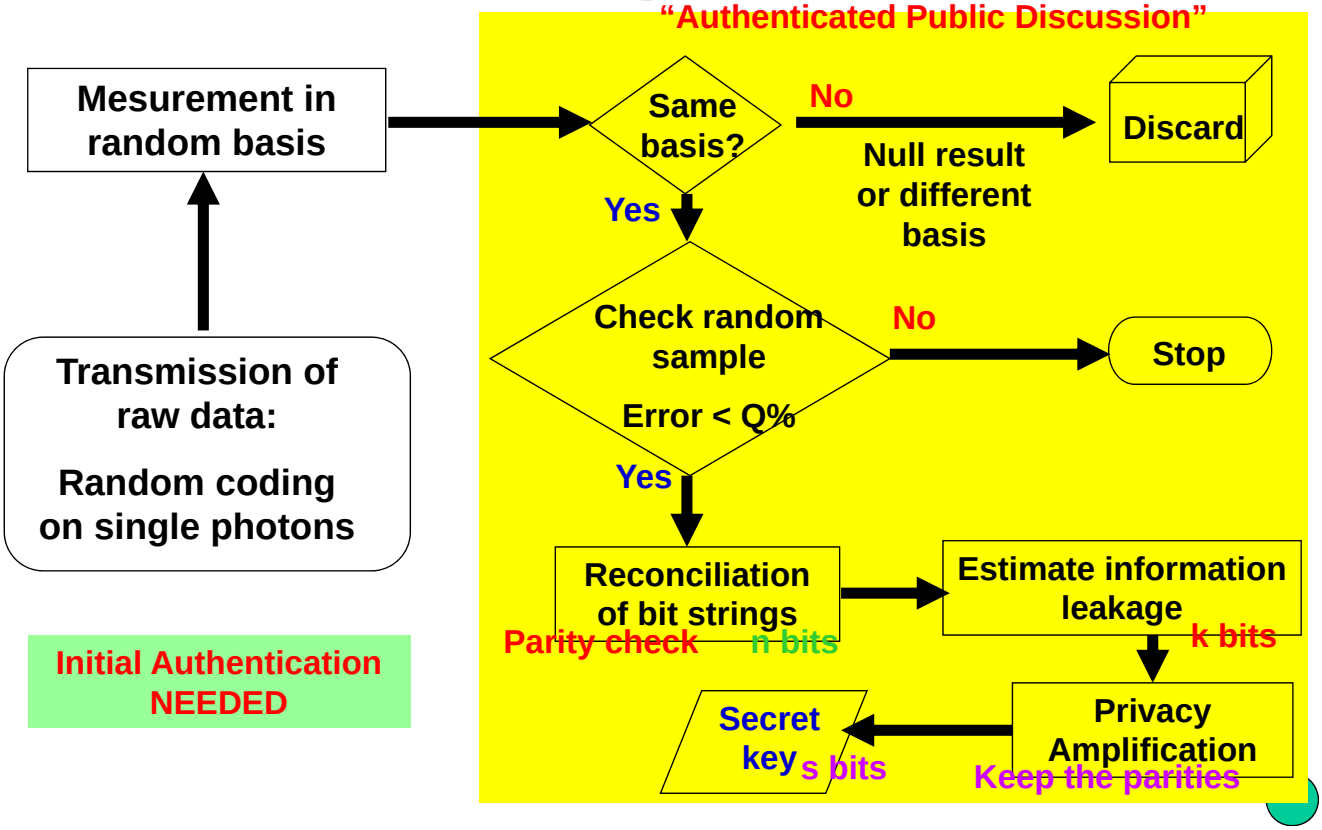
- **Alice**

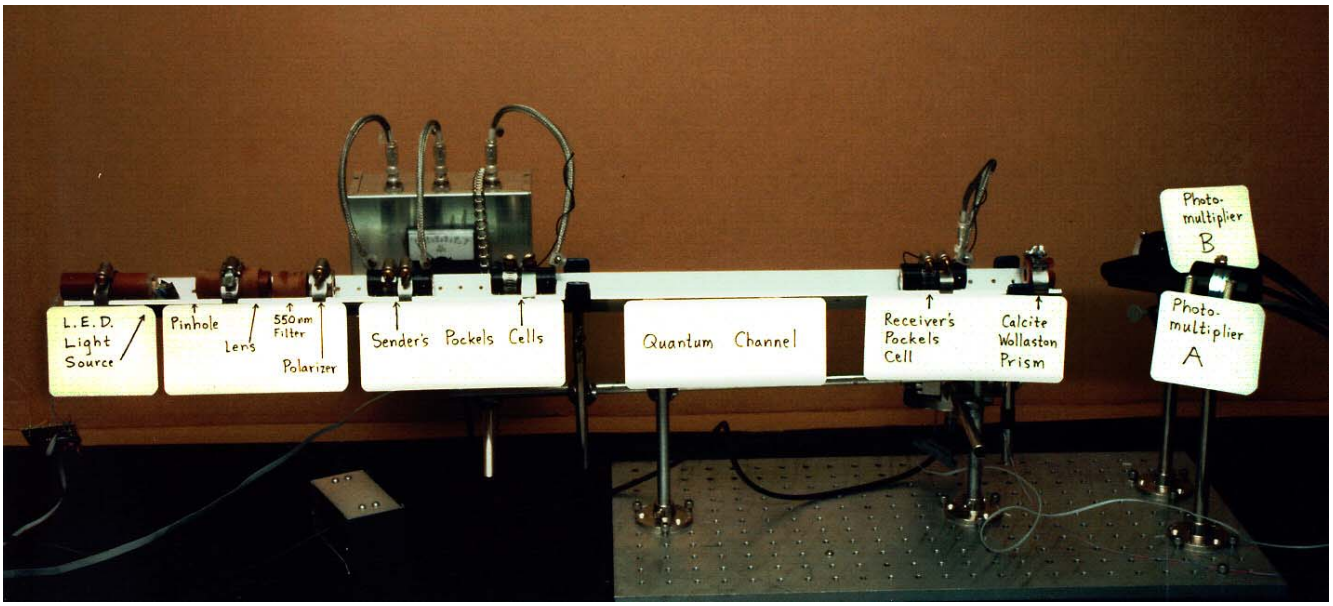
A1 =	0	1	1	0	0	1	0	0	0	0	1	1
A2 =	⊗	⊕	⊗	⊕	⊗	⊕	⊗	⊕	⊗	⊕	⊗	⊕
P =	⤢	↕	⤡	↔	⤢	↕	⤢	↔	⤢	↔	⤡	↕

- **Bob**

B =	⊕	⊕	⊕	⊗	⊕	⊕	⊗	⊗	⊕	⊕	⊗	⊕
D =	0	1	0	0	0	1	0	0	0	0	1	1
	1		1	1	1			1	1			

BB84 full implementation

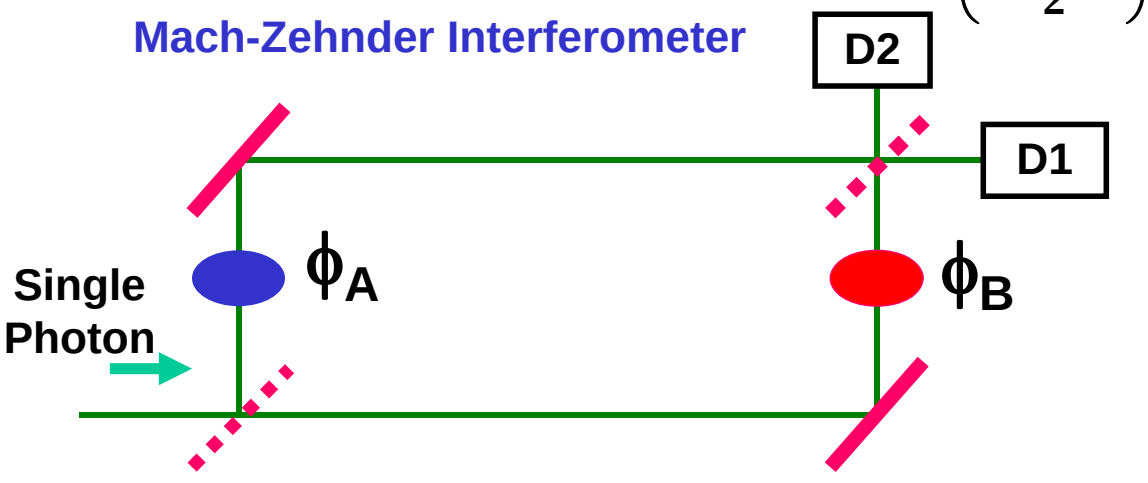




World's first QKD (1989): Bennett(IBM) et al.
32 cm in free space with 4 polarizations

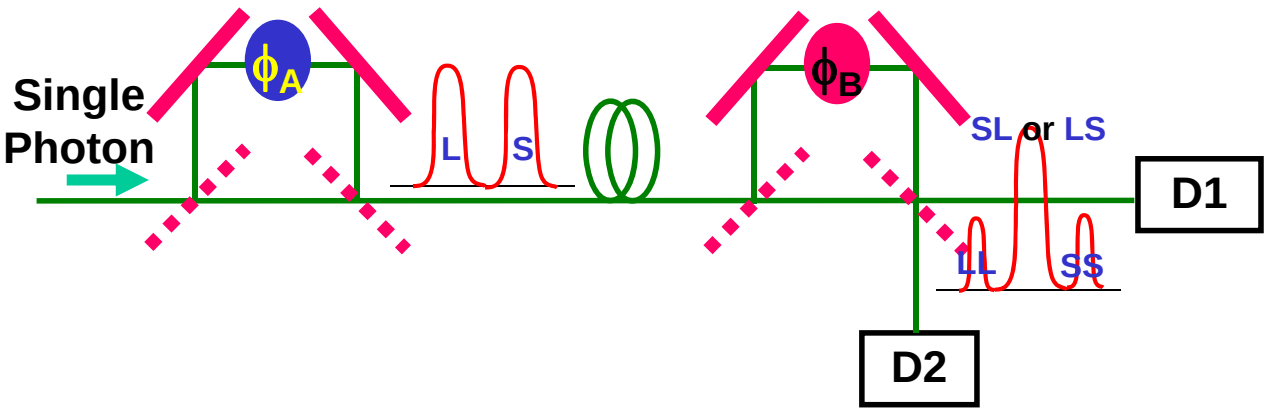
Phase Coding

$$\sin^2\left(\frac{\phi_A - \phi_B}{2}\right)$$



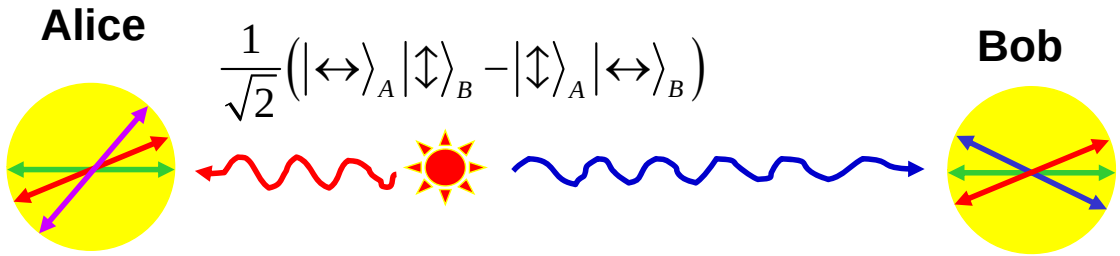
Cf. Delayed Choice (Wheeler)

Phase Coding



QKD via QE

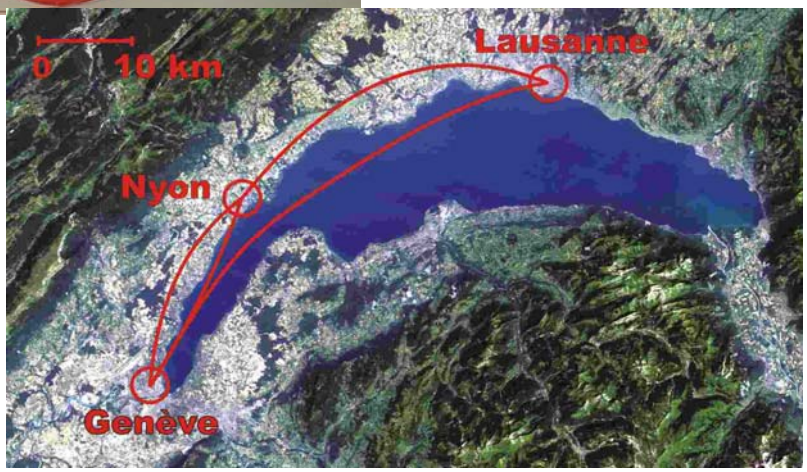
Ekert 91



- Measurement of same polarization: Anticorrelation
- Measurement of different polarization :
  Bell's Inequality to check the eavesdropping

Quantum Key Distribution over 67 km with a plug&play system

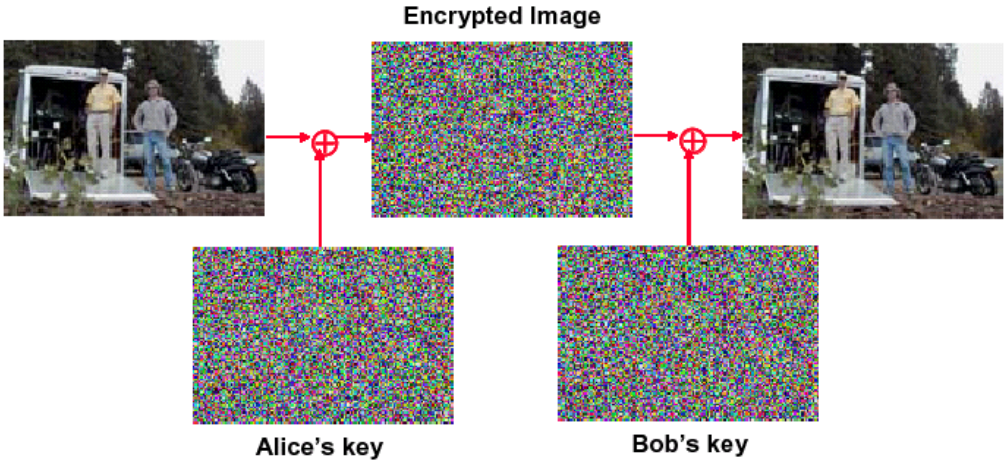
Gisin, Zbinden, QP/0203118



Practical free-space quantum key distribution over 10 km in daylight and at night

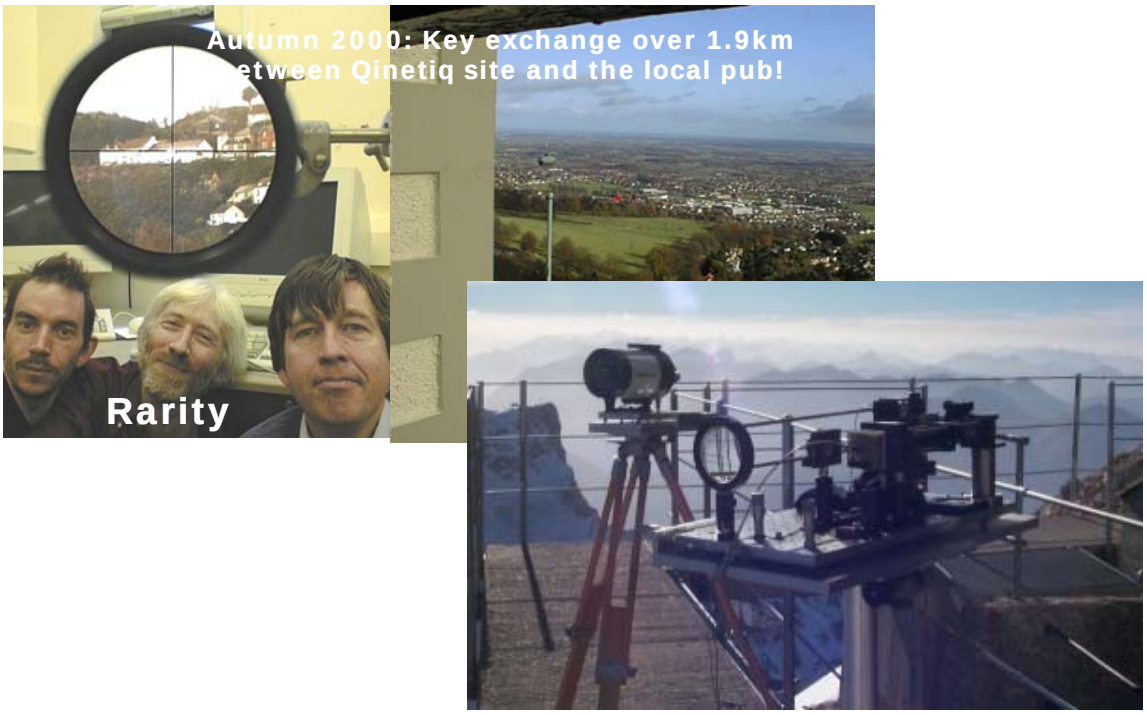
30km 45km

Richard J. Hughes, Jane E. Nordholt, Derek Derkacs and Charles G. Peterson **QP/0206092**

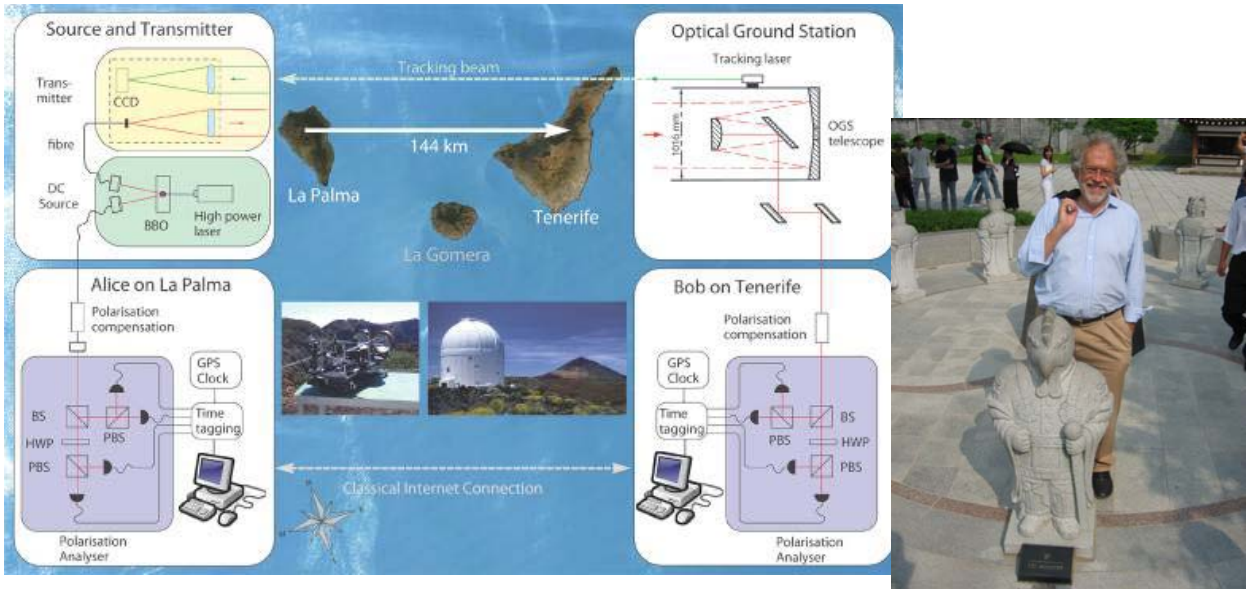


http://www.eqcspot.org/

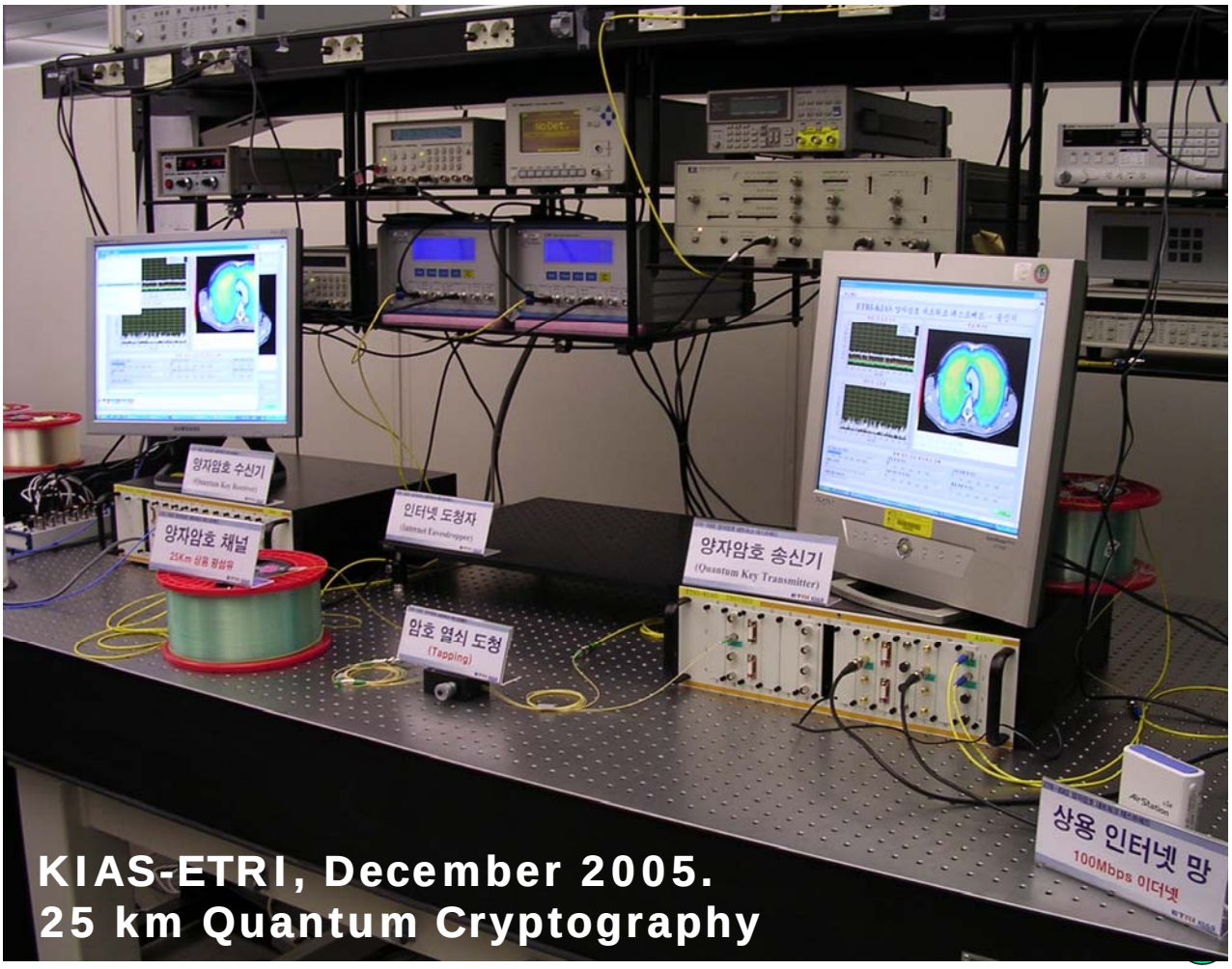
Autumn 2001: 23.4km Qinetiq-MPQ joint free space key exchange trial between Zugspitze and Karwendel



144 km free-space, Zeilinger (2007)



AQIS 2008 hosted by KIAS



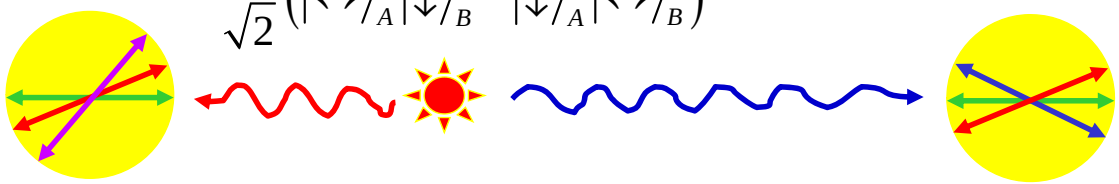
KIAS-ETRI, December 2005.
25 km Quantum Cryptography

Quantum Key Distribution

Entanglement Scheme Ekert 91

Alice **Bob**

$$\frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle_A|\updownarrow\rangle_B - |\updownarrow\rangle_A|\leftrightarrow\rangle_B\right)$$



- **Same Polarization: Anticorrelation**
- **Different Polarization: Bell's Inequality to check the eavesdropping**
- **Entanglement Purification**

Quantum Repeater

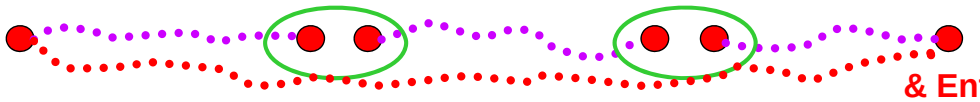
1. Quantum Repeater

~100 km → Indefinite distance

Briegel, Durr, Cirac, and Zoller, quant-ph/9803056

Transmission: Photon

Storage, Processing: Atomic Physics, etc.



& Entanglement Purification

2. Multiuser Quantum Network

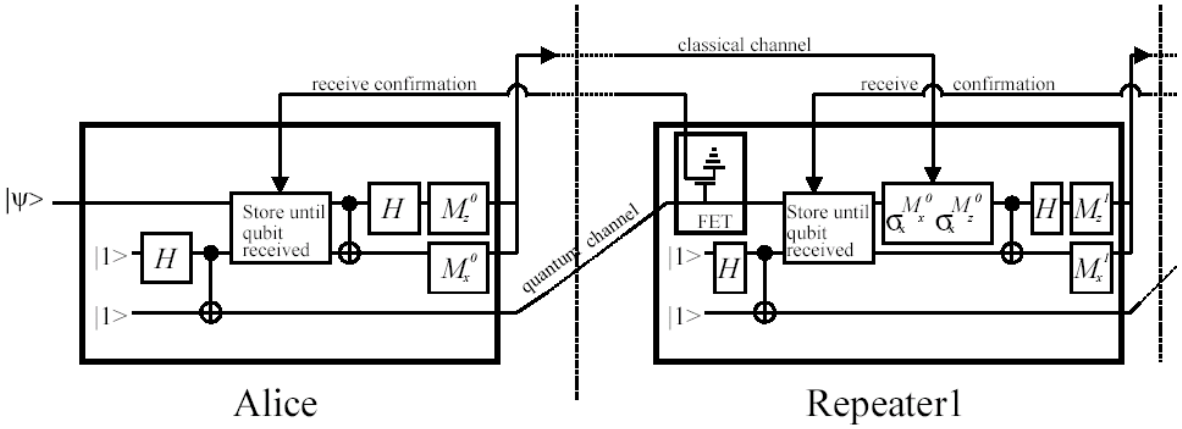
1:1 → multiusers

Phoenix, Barnett, Townsend, and Blow, JMO 42, 1155 (1995)

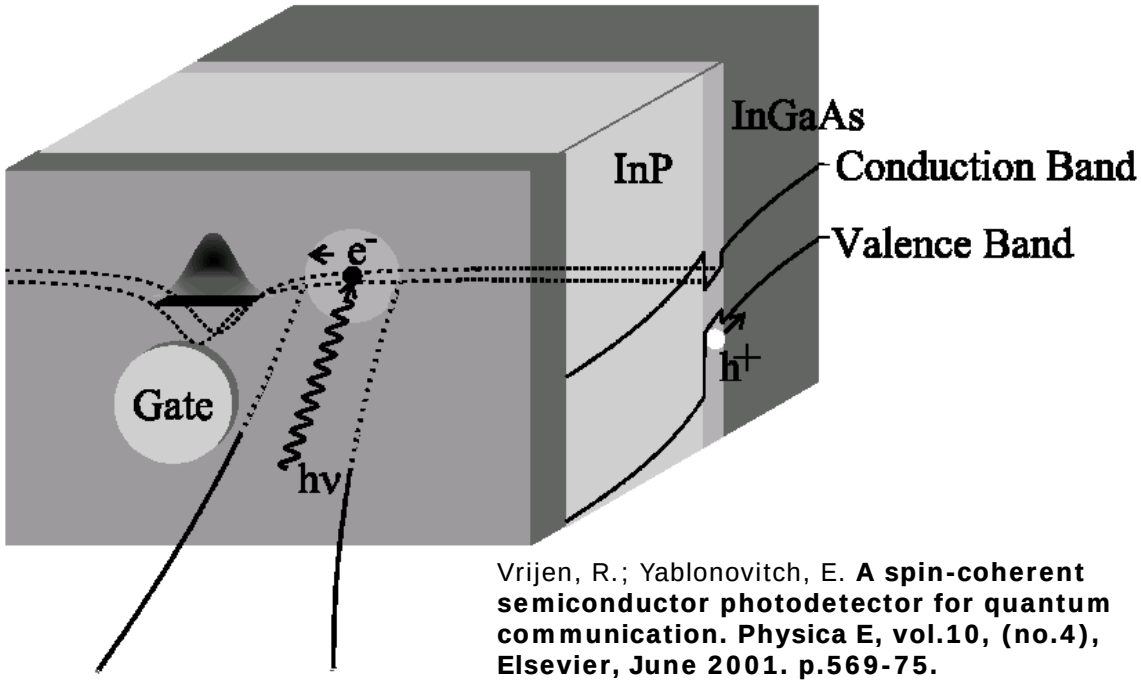
Biham, Huttner, and Mor, Phys. Rev. A 54, 2651 (1996)

Quantum Repeater

Vrijen, R.; Yablonovitch, E. **A spin-coherent semiconductor photodetector for quantum communication. Physica E, vol.10, (no.4), Elsevier, June 2001. p.569-75.**



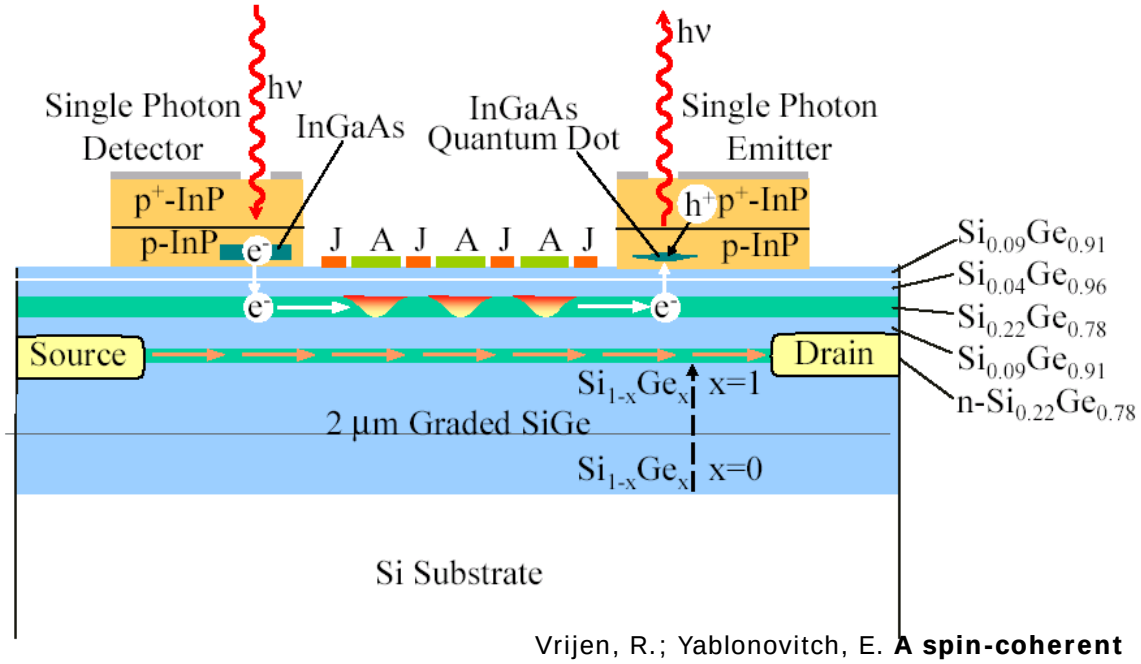
Yablonovitch



Vrijen, R.; Yablonovitch, E. **A spin-coherent semiconductor photodetector for quantum communication. Physica E, vol.10, (no.4), Elsevier, June 2001. p.569-75.**

Entanglement Preserving Spin-Coherent Semiconductor Photodetector

Yablonovitch

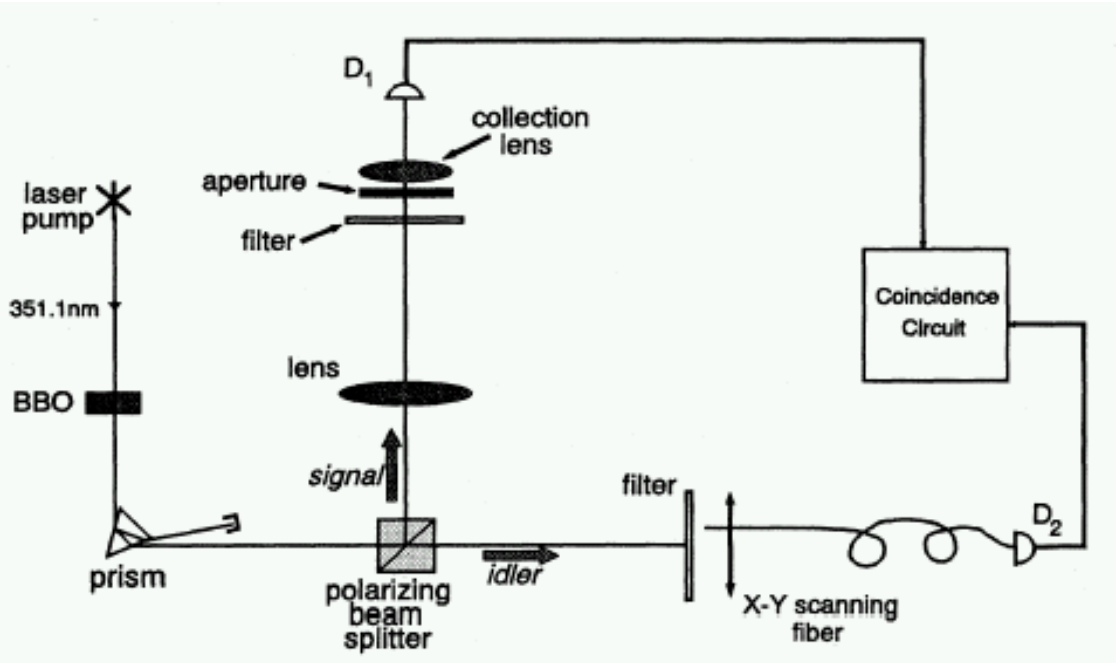


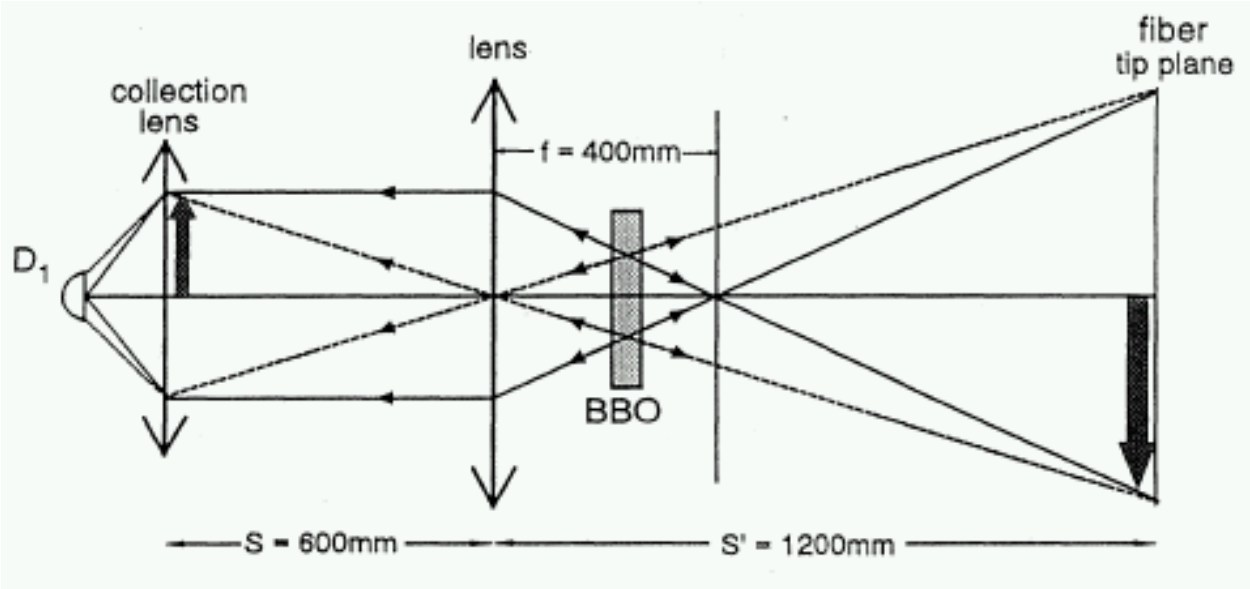
Vrijen, R.; Yablonovitch, E. **A spin-coherent semiconductor photodetector for quantum communication. Physica E, vol.10, (no.4), Elsevier, June 2001. p.569-75.**

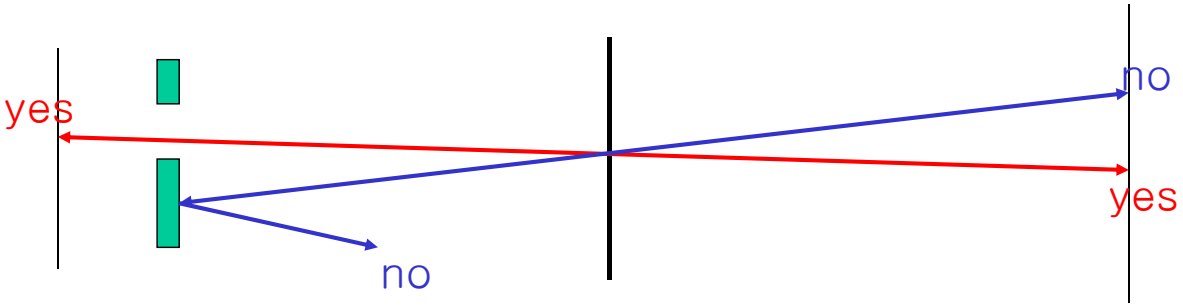
Yablonovitch

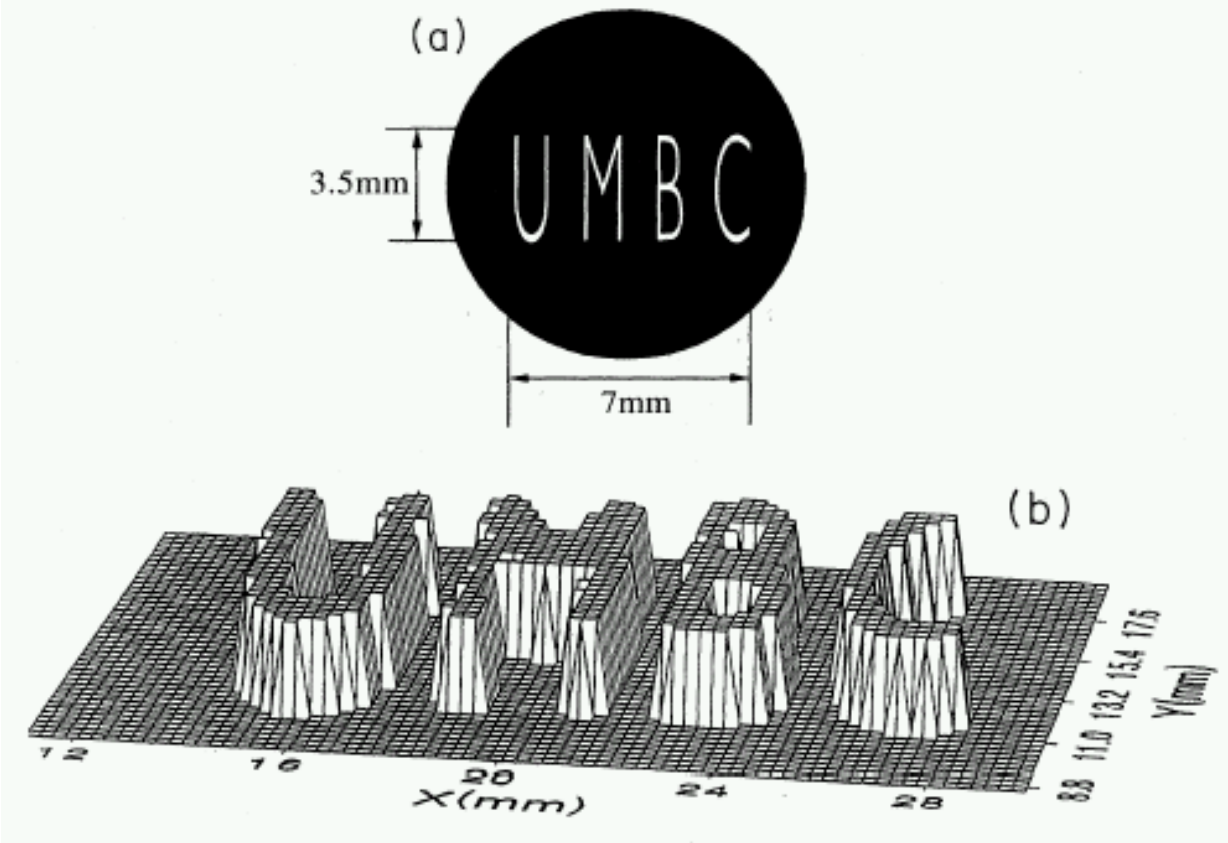
Optical Imaging by Two-Photon Entanglement

Shih *et al*., PRA52, R3429 (1995).



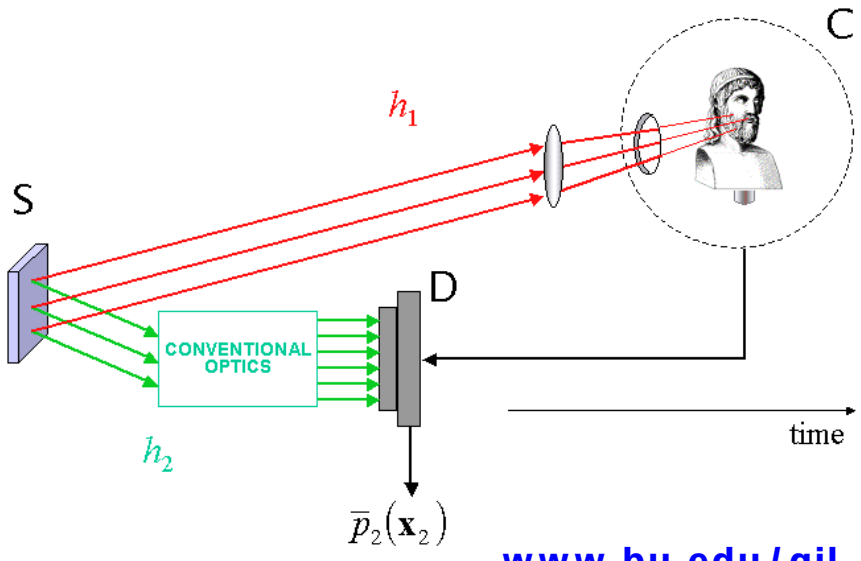






Quantum Holographic Imaging

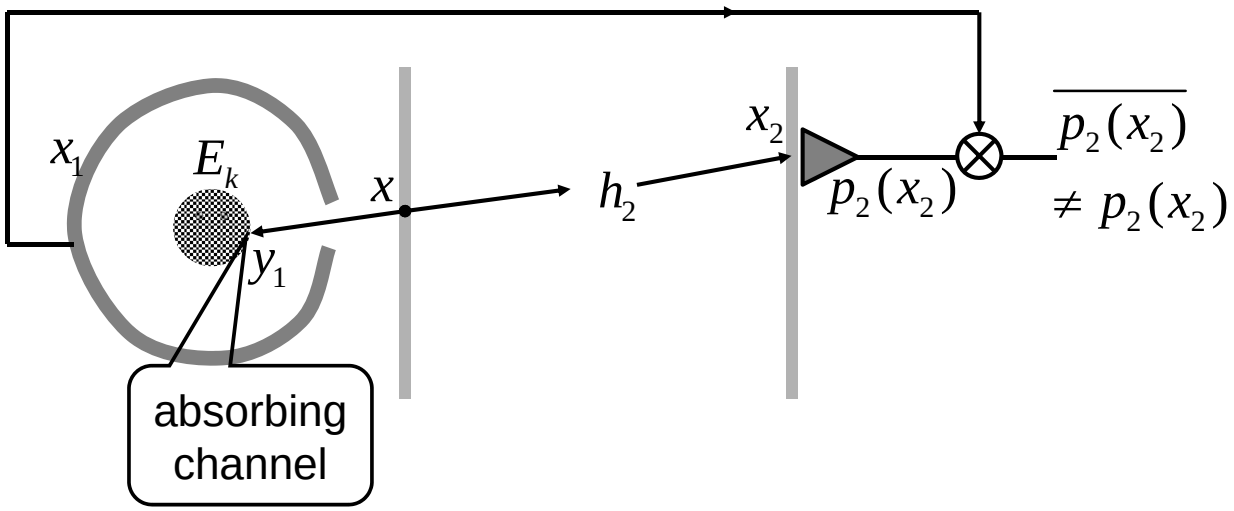
(Saleh et al. at Boston University)



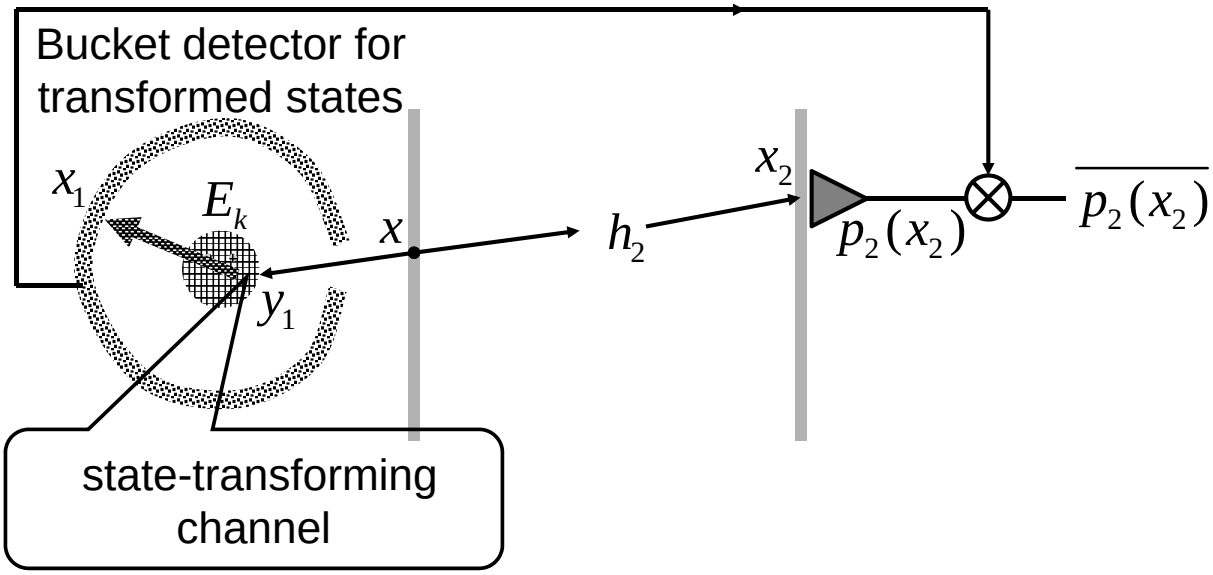
www.bu.edu/qil

PRL 87, 123602 (Sep 2001); Optics Express 9, 498 (Nov 2001)

Complementary image of absorbing channel



With state-transforming channels,



Quantum Lithography

September 20, 2001

WHAT'S NEXT

Quantum Theory Could Expand the Limits of Computer Chips

By ANNE EISENBERG

Using principles of quantum theory to manipulate light is the stuff of rarefi research, not the factory floor. But quantu theory may turn out to have surprisingly practical applications in manufacturing fa computer chips.

Dr. Shih's work follows a theoretical paper published in June 2000 in Physical Review Letters proposing that entangled pairs of photons be used to focus light to regions smaller than those achievable by individual photons, thus making them useful in lithographic processes.

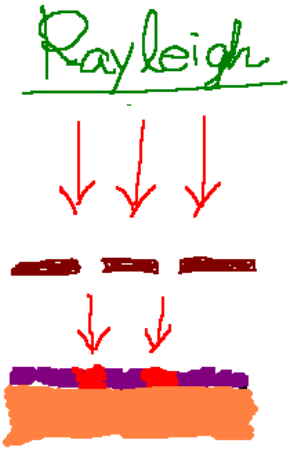
Dr. Jonathan Dowling, a physicist at NASA's Jet Propulsion Laboratory at the California Institute of Technology in Pasadena, Calif., and one of the authors of the theoretical paper, said he was very relieved to read Dr. Shih's results. "I'm a theorist," Dr. Dowling said, "so when I predict an effect that hasn't been seen, there's always a nagging doubt that it won't agree with the experimental data. This is the first proof that the prediction is legitimate."

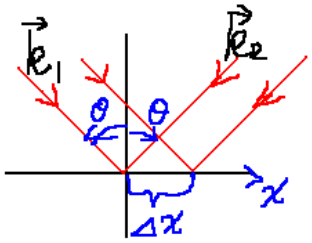
The Shih paper is important, Dr. Dowling said, because "if we can halve the space betwe features on chips, we can put twice as many features in the X dimension and twice as ma the Y dimension." This might mean that four times as many circuits might be placed on a

Entangled photons like the ones used by Dr. Shih's group could be produced in a laborat passing a light beam through a special crystal, and in other ways. In the Shih experiment, entangled photons were created by shining an argon laser beam through the crystal.

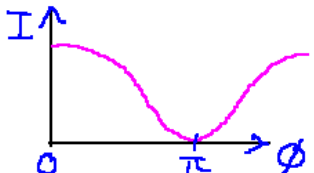
What's Next: It's Still Gray Box, but the Inn Are Changing (Augus 2001)

OTHER RESOURCES
Newsletters
Subscribe to Circuits
Sign up to receive a fi weekly Circuits news e-mail, with technolo and tips and exclusive commentary by Davic the State of the Art co





$$2k\Delta x \sin\theta = \phi$$



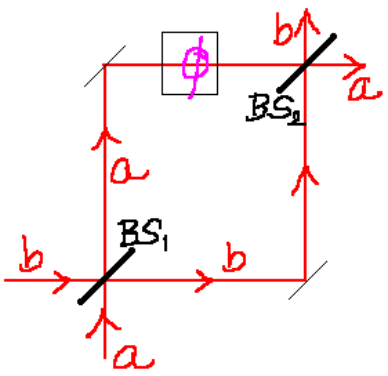
$$0 \quad \frac{\pi}{2k\sin\theta} = \frac{\lambda}{4\sin\theta} = \Delta x$$

$$I \propto \left| e^{i\vec{k}_1\cdot\vec{r}} + e^{i\vec{k}_2\cdot\vec{r}} \right|^2$$

$$= \left| 1 + e^{i\underbrace{(\vec{k}_2-\vec{k}_1)\cdot\vec{r}}_{\equiv\phi}} \right|^2$$

$$= 4\cos^2\frac{\phi}{2}$$

Mach-Zehnder Interferometer



$$|1\rangle_a|0\rangle_b \equiv |10\rangle = a^\dagger|00\rangle$$

$$\xrightarrow{BS_1} B a^\dagger B^\dagger B|00\rangle = \frac{1}{\sqrt{2}}(a^\dagger + b^\dagger)|00\rangle$$

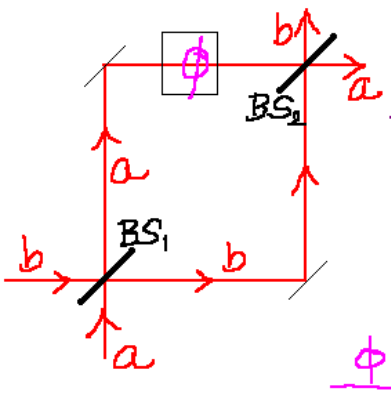
$$\xrightarrow{\phi} \frac{1}{\sqrt{2}}(e^{i\phi}a^\dagger + b^\dagger)|00\rangle$$

$$\xrightarrow{BS_2} \frac{1}{\sqrt{2}}\left(e^{i\phi}\frac{1}{\sqrt{2}}(a^\dagger+b^\dagger) + \frac{1}{\sqrt{2}}(-a^\dagger+b^\dagger)\right)|00\rangle$$

Amplitude of $|1\rangle_a|0\rangle_b = a^\dagger|00\rangle$; $e^{i\phi} - 1$

$I \propto |1 - e^{i\phi}|^2$!!! Rayleigh

TWO-PHOTON ABSORPTION YABLONOVITCH



incoherent input!

$$|2\rangle_a|0\rangle_b \equiv |20\rangle = \frac{(a^\dagger)^2}{\sqrt{2}}|00\rangle$$

$$\xrightarrow{BS_1} \frac{1}{\sqrt{2}}\frac{1}{2}(a^\dagger+b^\dagger)(a^\dagger+b^\dagger)|00\rangle$$

$$= \frac{1}{2\sqrt{2}}(a^{\dagger 2} + 2a^\dagger b^\dagger + b^{\dagger 2})|00\rangle$$

$$\xrightarrow{\phi} \frac{1}{2\sqrt{2}}(e^{2i\phi}a^{\dagger 2} + e^{i\phi}2a^\dagger b^\dagger + b^{\dagger 2})|00\rangle$$

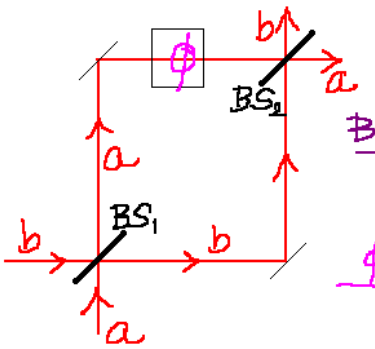
$$\xrightarrow{BS_2} \frac{1}{2\sqrt{2}}\left\{e^{2i\phi}\frac{1}{2}(a^{\dagger 2}+b^{\dagger 2}+2a^\dagger b^\dagger) + e^{i\phi}(-a^{\dagger 2}+b^{\dagger 2}) + \frac{1}{2}(a^{\dagger 2}+b^{\dagger 2}-2a^\dagger b^\dagger)\right\}|00\rangle$$

[amplitude of $|2\rangle_a|0\rangle$] $\propto \frac{1}{2}e^{2i\phi} - e^{i\phi} + \frac{1}{2}$

$I_{TPA} \propto |e^{2i\phi} - 2e^{i\phi} + 1|^2$

TWO-PHOTON ENTANGLEMENT & TPA

DOWLING



$|1\rangle_a|1\rangle_b = a^\dagger b^\dagger |00\rangle$

$BS_1 \rightarrow \frac{1}{2}(a^\dagger + b^\dagger)(-a^\dagger + b^\dagger)|00\rangle = \frac{1}{2}(-a^{\dagger 2} + b^{\dagger 2})|00\rangle = \frac{1}{\sqrt{2}}(-|20\rangle + |02\rangle)$

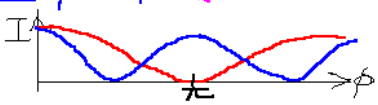
$\phi \rightarrow \frac{1}{\sqrt{2}}(-e^{2i\phi}|20\rangle + |02\rangle)$

$= \frac{1}{2}(-e^{2i\phi} a^{\dagger 2} + b^{\dagger 2})|00\rangle$

$BS_2 \rightarrow \frac{1}{2}\{-e^{2i\phi}\frac{1}{2}(a^{\dagger 2} + b^{\dagger 2} + 2a^\dagger b^\dagger) + \frac{1}{2}(a^{\dagger 2} + b^{\dagger 2} - 2a^\dagger b^\dagger)\}|00\rangle$

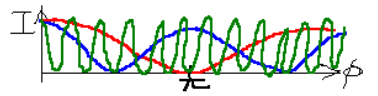
TWO-PHOTON ABSORPTION ... $|20\rangle$;

$I_{TPA} \propto |1 - e^{2i\phi}|^2 = 4\sin^2\phi$ vs. $\cos^2\frac{\phi}{2}$



N-Photon Absorption with $|N0\rangle + |0N\rangle$

$|e^{iN\phi} + 1|^2$



Quantum Interferometric Optical Lithography: Exploiting Entanglement to Beat the Diffraction Limit

Agedi N. Boto,1 Pieter Kok,2 Daniel S. Abrams,1 Samuel L. Braunstein,2 Colin P. Williams,1 and Jonathan P. Dowling1,* **PRL85, 2733 (2000)**

Two-Photon Diffraction and Quantum Lithography

Milena D'Angelo, Maria V. Chekhova,* and Yanhua Shih **PRL87, 13602 (2001)**

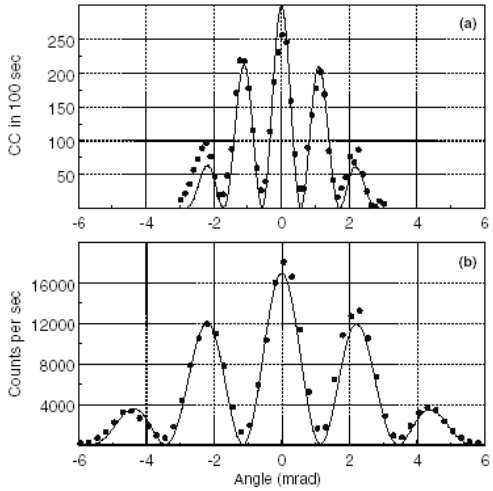


FIG. 3. (a) Experimental measurement of the coincidences for the two-photon double-slit interference-diffraction pattern. (b) Measurement of the interference-diffraction pattern for classical light in the same experimental setup. With respect to the classical case, the two-photon pattern has a faster spatial interference modulation and a narrower diffraction pattern width, by a factor of 2.

Quantum Metrology

We are applying our understanding of the quantum nature of entangled-photon pairs for the characterization of optical-detector quantum efficiency, source radiation density, and photonic-material characteristics, all without the necessity of employing a reference. The use of this unique light source provides particular advantages over the classical counterparts that are traditionally used. Another example is provided by a technique we call quantum ellipsometry. The high accuracy required in traditional ellipsometric measurements necessitates the absolute calibration of both the source and the detector. These requirements can be circumvented by using spontaneous parametric down-conversion in conjunction with a novel polarization interferometer and coincidence-counting detection scheme.

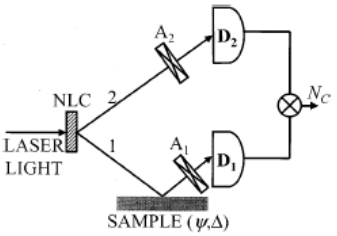


Fig. 3. Entangled twin-photon ellipsometer.

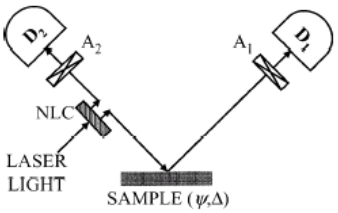


Fig. 4. Unfolded version of the entangled twin-photon ellipsometer displayed in Fig. 3.

Entangled-photon ellipsometry

A. F. Abouraddy, K. C. Toussaint, Jr., **A. V. Sergienko, B. E. A. Saleh, and M. C. Teich**
J. Opt. Soc. Am. B. **19**, 656-662 (2002). [PDF]

Ellipsometric measurements by use of photon pairs generated by spontaneous parametric downconversion

Ayman F. Abouraddy, Kimani C. Toussaint, Jr., Alexander **V. Sergienko, Bahaa E. A. Saleh, and Malvin C. Teich**
Opt. Lett. **26**, 1717-1719 (2001). [PDF]

(from Michael Brooks)

Quantum Information Processing

Roadmap (1987-1998)

Research Goals

Basic Research

- Quantum interference
- Ion traps
- Cavity QED
- Quantum dots
- NMR schemes
- Si:P
- Shor's algorithm
- Quantum cryptography
- Grover's algorithm
- Single photon detector
- Error correction

Applications

Now

- Photon counters
- Precision range finding
- Optical time-domain reflectometry
- Metrology
- Secure optical communications

Quantum Information Processing
Roadmap (1998-2003)

Research Goals

Near Term Goals
- NMR to do 8 qubit QC
- 3-5 photon entanglement
- 3-5 qubit ion trap
- Quantum dot gate
- Silicon-based gate
- Few qubit applications
- New algorithms
- Fault tolerant QC
- Novel QC
- Quantum repeaters
- Quantum amplifiers
- Detectors
- Sources

Applications

Near Future
- Quantum cryptography demonstrators
- General quantum communications
- Random number generators
- 2-photon metrology
- DNA sequencing
- Single molecule sensors
- Simulation of quantum systems
- Quantum gyroscopes

(from Michael Brooks)

Quantum Information Processing
Roadmap (2003-2015)

Research Goals

Mid Term Goals
- 10 - 20 qubit computation
- Demonstrator systems
- Novel algorithms
- Macroscopic superposition
- Bose condensate connections
- Quasi-classical few particle gates and bits

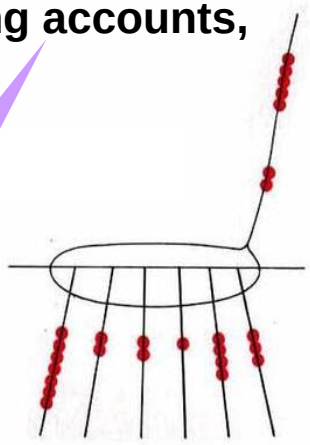
Applications

Far Future
- Quantum repeaters
- Quantum amplifiers
- Quantum computers
  - factoring
  - non-structured information retrieval
- Molecular simulation

QUIPU [kí:pu]

1. Quantum Information Processing Unit

2. A device consisting of a cord with knotted strings of various colors attached, used by the ancient Peruvians for recording events, keeping accounts, etc.

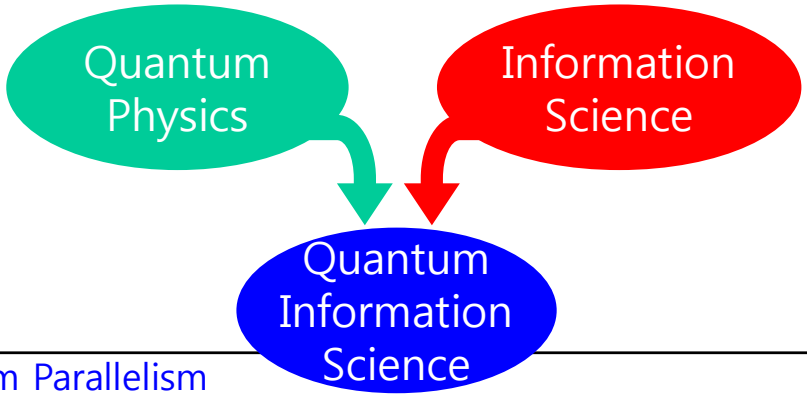


* Peruvian Information Processing Unit for Communication and Computation

Quantum Beyond Nano

"There's plenty of room at the bottom." -Feynman
Moore's Law :continue to shrink→ nanotechnology
→ meets quantum regime
→ uncertainty principle
uncertainty in bits (0's and 1's)

Quantum Technology
→ turns uncertainty into magic
Actively *utilizing quantumness*
'Let the quantum system solve
the quantum manybody problems' -Feynman



Quantum Parallelism

→ Quantum computing is
exponentially larger and faster than digital computing.
Quantum Fourier Transform, Quantum Database Search,
Quantum Many-Body Simulation (Nanotechnology)

No Clonability of Quantum Information,
Irrevesability of Quantum Measurement

→ Quantum Cryptography (Absolutely secure digital communication)

Quantum Correlation by Quantum Entanglement

→ Quantum Teleportation, Quantum Superdense Coding,
Quantum Cryptography, Quantum Imaging