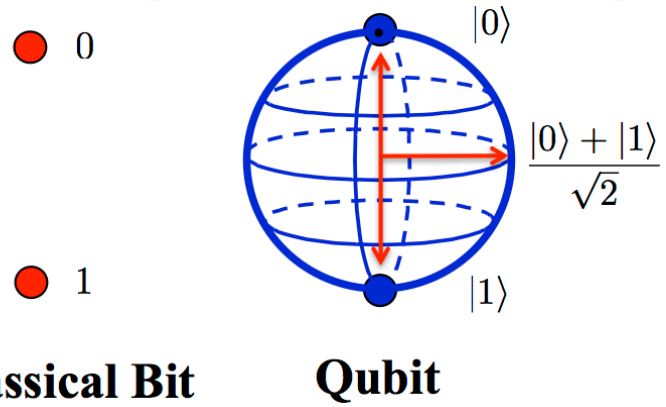
# Introduction to Quantum Computing/Networking and their Applications to Cybersecurity




**Raj Jain**
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@wustl.edu

These slides and video recording of this class lecture are available at:
http://www.cse.wustl.edu/~jain/cse5700-25/

**Student Questions**


©2025 Raj Jain



# Overview

1. What is a Quantum and Quantum Bit?
2. Matrix Algebra Review
3. Quantum Gates: Not, And, or, Nand
4. Applications of Quantum Computing
5. Quantum Hardware and Programming

## Student Questions


©2025 Raj Jain

# Selecting the Right Field



- An important question for **students**, academics, entrepreneurs, and companies
- Most academics follow the herd or stick to their old expertise.
- Goal: To impact

⇒ Follow the **paradigm shifts**:

- 2008: Next Generation Internet/SDN
- …
- 2025: Whatever is being **hyped** this yr?



- The United Nations has declared 2025 The International Year of Quantum Science and Technology, https://quantum2025.org

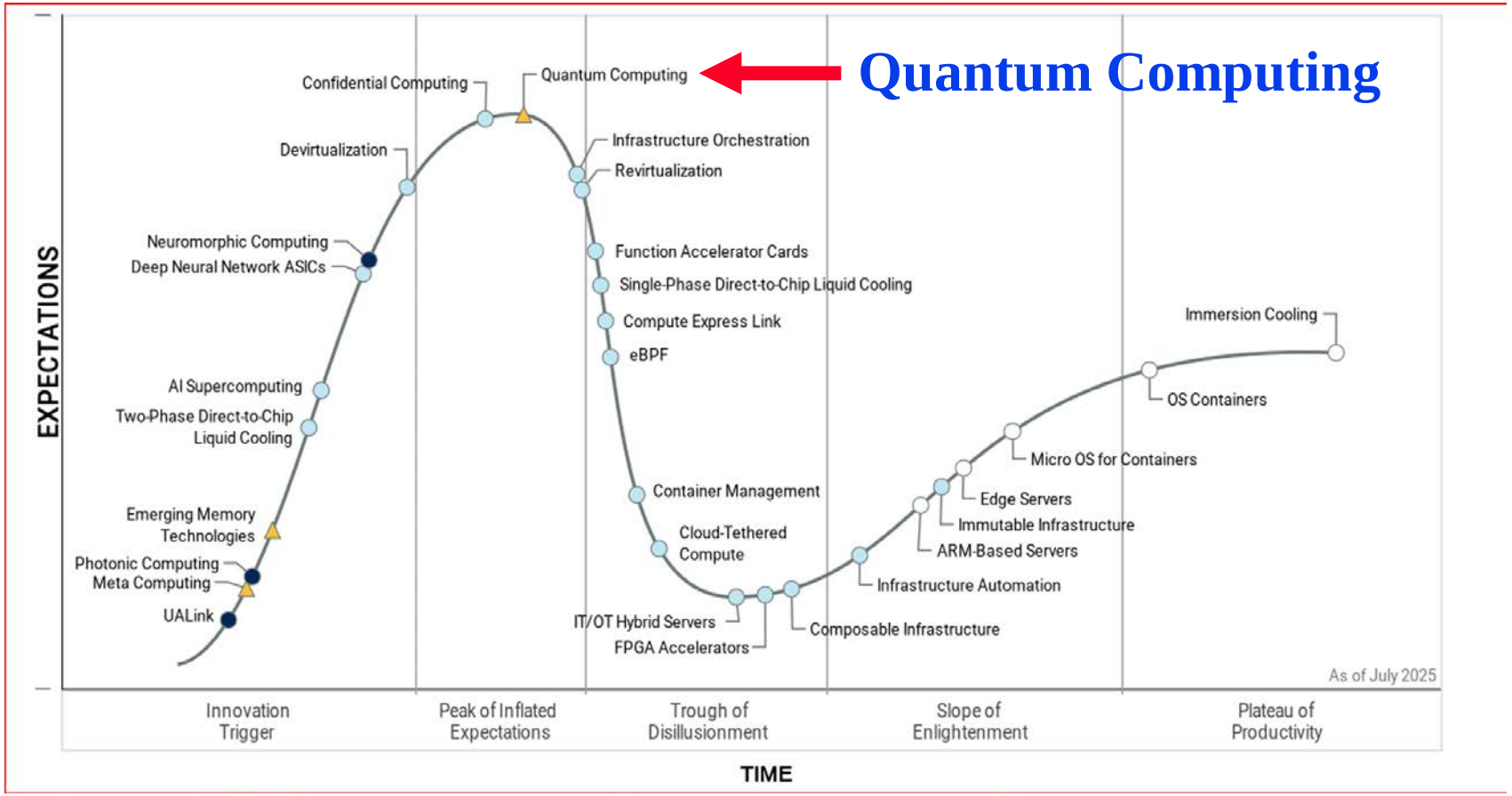
Industries adapt by necessity.

**Academics continue to develop deeper expertise in what they know.**

## Student Questions


©2025 Raj Jain

# Hype Cycle for Compute 2025




**This is the right time to get into Quantum.**

Ref: T. Harvey, "Hype Cycle for Compute, 2025," Gartner Report ID G00832015, July 1, 2025, 98 pp. (Available via subscription)

## Student Questions



©2025 Raj Jain

# Investment in Quantum

- $40-55 billion in the Asia-Pacific region (APAC)
- China alone accounts for $15 billion in public investment and
  - A $138B government-backed venture fund
  - University of Science and Technology of China (USTC) Chinese Academy of Sciences (CAS), National Development Reform Commission (NRDC)
- European Union (including Germany, France, and the UK) over $10B
- US Federal Government $5-6 B
- The private sector investments are many times more than the public expenditure above.
- Google, IBM, Microsoft, Amazon, and Cisco are all invested.

**Student Questions**


©2025 Raj Jain

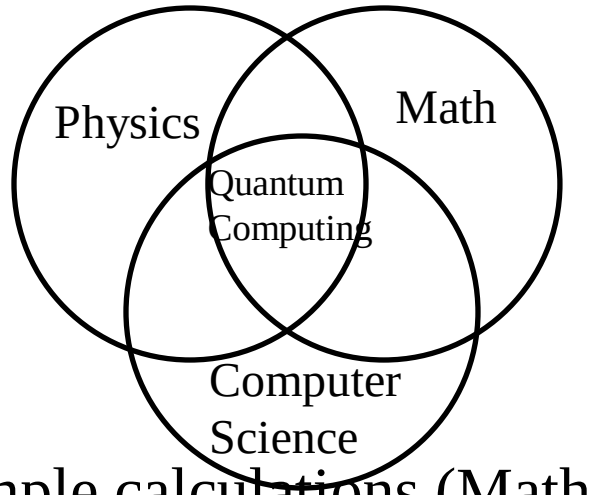
# US Investments in Quantum

- NIST, NSF, DOE, DOD, NASA, NSA, and IARPA (Intelligence ARPA) – all coordinated by the National Quantum Coordination Office (NQCO).
- Illinois has set up a Quantum Park in Chicago. Has invited Cisco, IBM, Google, and other companies to set up there.
- **DC-Qnet:**
  - A Consortium of US government agencies in the Washington DC area: NIST, NRL. ARL, USNO, NSA, NASA, and AFRL.
  - Goal: to build and operate a functional quantum network
  - Uses existing fiber network over metropolitan distances
- Other testbeds: DOE's Quantum Garage, QUIET/LOUD facilities, and NSF's National Quantum Nanofab (NQN)

**Student Questions**


©2025 Raj Jain

# Pre-Requisite for Quantum Networking



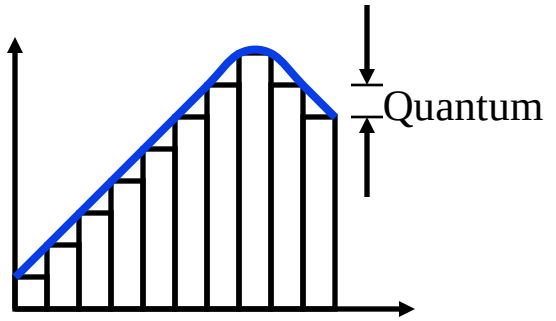

1. **Probability**: simple calculations (Math 326 of Math 3200)
2. **Complex numbers**: Real and Imaginary parts
3. **Linear Algebra**: Row and column vectors, Matrix multiplication, Inverse of a Matrix, Eigen Vectors, Eigen Values, Linear System of Equation (Math 309)
4. **Boolean Algebra and Logic**: AND, OR, XOR, NAND, etc. (CSE 132, CSE240, CSE 260M)

**Student Questions**


©2025 Raj Jain

# What is a Quantum?

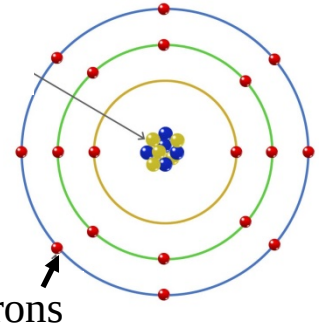
- Quantization: Analog to digital conversion
- Quantum = Smallest discrete unit
- **Wave Theory**: Light is a wave. It has a frequency, phase, amplitude
- **Quantum Mechanics**: Light behaves like discrete packets of energy that can be absorbed and released
- **Photon** = One quantum of light energy
- Photons can move an electron from one energy level to next higher level
- Photons are released when an electron moves from one level to lower energy level









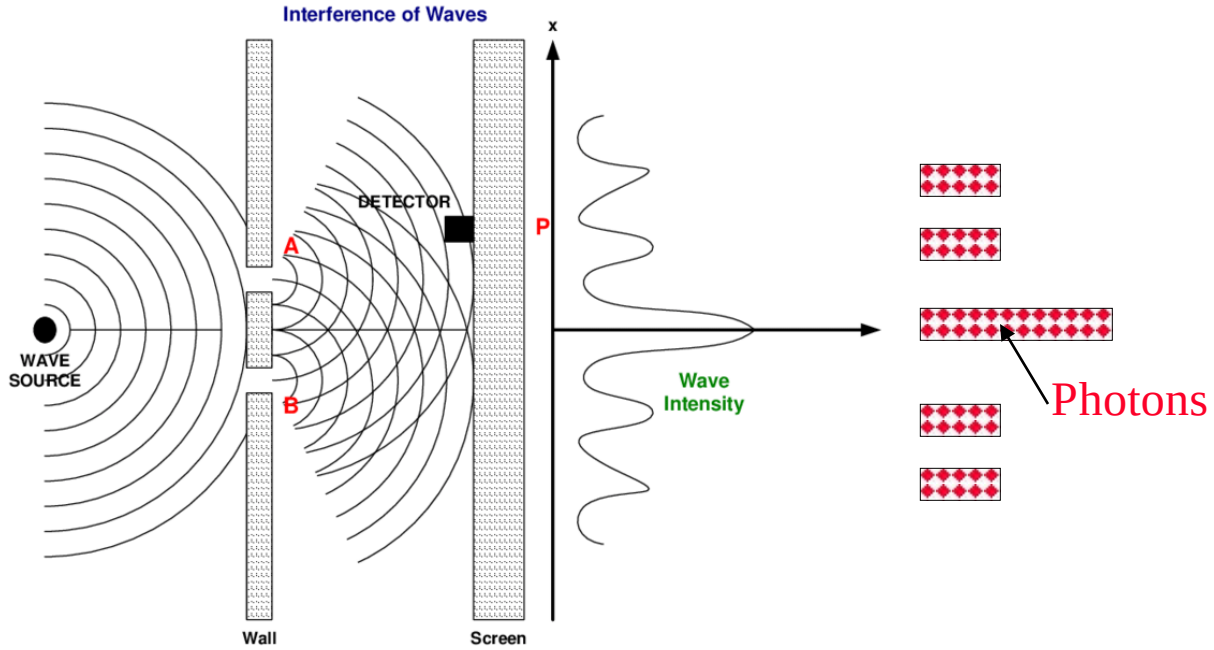




**Student Questions**


©2025 Raj Jain

# Are Photons Particles or a Wave?

- Young's Double-Slit Experiment 1801




- The two waves exiting the slits interfere.
- Einstein showed that light consists of photon particles.
- Photons are both particles and waves. Electrons are both too?

**Student Questions**



©2025 Raj Jain

# Quantum Bits

1. Computing bit is a binary scalar: 0 or 1
2. Quantum bit (**Qubit**) is a 2×1 **vector**, e.g., $\begin{bmatrix}1\\0\end{bmatrix}$ or $\begin{bmatrix}0\\1\end{bmatrix}$ or $\begin{bmatrix}\alpha\\\beta\end{bmatrix}$
3. **Dirac Notion: Ket-Zero** $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ **Ket-One** $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$

   Ket-Psi = $|\psi\rangle = \begin{bmatrix}\alpha\\\beta\end{bmatrix}$
3. Qubits are probabilistic. Elements represent probability amplitude.
4. **Probability** of each element in a qubit vector is proportional to the square of the element:
   Probability of $\begin{bmatrix}\alpha\\\beta\end{bmatrix}$ being 0: $\frac{\alpha^2}{\alpha^2+\beta^2}$ Probability of $\begin{bmatrix}\alpha\\\beta\end{bmatrix}$ being 1: $\frac{\beta^2}{\alpha^2+\beta^2}$
5. Example: Probability of $\begin{bmatrix}0\\1\end{bmatrix}$ being 0 is $= \frac{0^2}{0^2+1^2} = \frac{0}{0+1} = 0$
   Probability of $\begin{bmatrix}0\\1\end{bmatrix}$ being 1 is $= \frac{1^2}{0^2+1^2} = \frac{1}{0+1} = 1$
6. Exercise: What is the probability of $\begin{bmatrix}1\\0\end{bmatrix}$ being 0 and 1?

   What is the probability of $\begin{bmatrix}0.6\\0.8\end{bmatrix}$ being 0 and 1?

**Student Questions**

End of Part 1


©2025 Raj Jain

# Complex Numbers

1. 1, 2, 3, 4, 5, are all **real numbers**
2. Square root: $\sqrt{100} = \sqrt{4 \times 25} = \sqrt{4} \times \sqrt{25} = 2 \times 5 = 10$
3. Square root of $\sqrt{-100} = \sqrt{4 \times 25 \times -1} = \sqrt{4} \times \sqrt{25} \times \sqrt{-1} = 2 \times 5 \times i = 10i$

   This is an **imaginary number**.
4. A combination of real number and imaginary number is a **complex number**, e.g., $1+2i$
5. **Addition** of complex numbers: Add the real and imaginary parts separately: $(1+2i) + (2+3i) = 3+5i$
6. **Multiplication** of Complex numbers: $(1+2i)(2+3i)$ $=1(2+3i)+2i(2+3i) = 2+3i+4i+6i^2 = 2 +7i-6 = -4+7i$

**Student Questions**


©2025 Raj Jain


End of Part 1

# Complex Numbers (Cont)

7. **Conjugate** of a complex number $x+iy$ is $x-iy$.
   E.g., conjugate of 2+3i is 2-3i. Conjugate of 1-2i is 1+2i.
8. **Modulus** |x+iy| of a Complex Number $x+iy$ is the square root of the product of the number by its conjugate:

$$\sqrt{(x+iy)(x-iy)} = \sqrt{x^2-(iy)^2} = \sqrt{x^2+y^2}$$

Example: $|3+4i| = \sqrt{3^2+4^2} = \sqrt{9+16} = \sqrt{25} = 5$

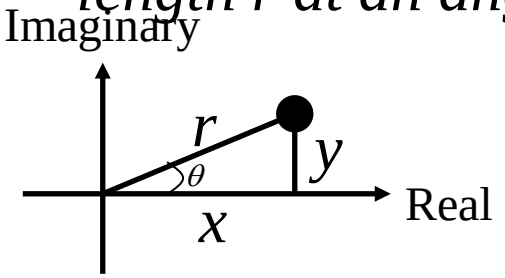
**Student Questions**


©2025 Raj Jain

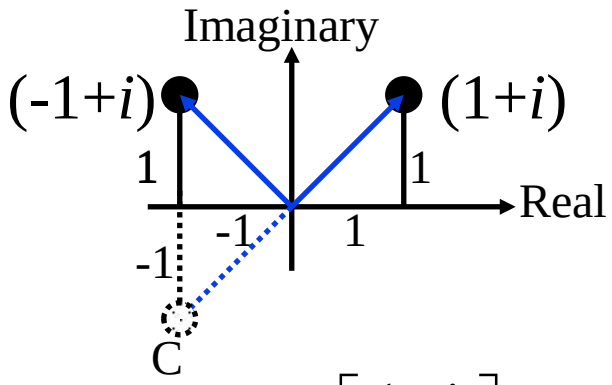

End of Part 1

# Polar Representation

- Complex numbers in 2D *can be represented as a vector of length r at an angle $\theta$ from the real axis.*




$$(x+iy) = re^{i\theta}$$
$$= r(cos(\theta) + isin(\theta))$$
$$r = \sqrt{x^2+y^2}$$
$$\theta = tan^{-1}(y/x)$$




$2\pi = 360^o$

$\pi/4 = 45^o$

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1+i\\-1+i\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}\sqrt{2}e^{i\pi/4}\\\sqrt{2}e^{3i\pi/4}\end{bmatrix} = \begin{bmatrix}e^{i\pi/4}\\e^{3i\pi/4}\end{bmatrix} = \begin{bmatrix}(\cos(\pi/4)+i\sin(\pi/4))\\(\cos(3\pi/4)+i\sin(3\pi/4))\end{bmatrix}$$

$\cos(\pi/4) = \frac{1}{\sqrt{2}}$ $\sin(\pi/4) = 1$

- **Exercise**: Find the complex and polar representation of C

## Student Questions



©2025 Raj Jain

# Dirac Bra-Ket Notation

- The vector $\psi$ is denoted in bra-kets $|\psi>$
- Brackets: { }, [ ], < >
- Bra <a|
- Ket |a>
- Example: Ket-zero and ket-one

$$\begin{bmatrix}1\\0\end{bmatrix} = |0> \quad \begin{bmatrix}0\\1\end{bmatrix} = |1>$$

- Bra is the transpose of the complex-conjugate of a Ket.
  Example: Bra-zero and Bra-one

$$\begin{bmatrix}1 & 0\end{bmatrix} = <0| \quad \begin{bmatrix}0 & 1\end{bmatrix} = <1|$$

**Student Questions**


©2025 Raj Jain

# Superposition

- The qubit $\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$ has a probability $\frac{\alpha^2}{\alpha^2+\beta^2}$ being measured in |0> state and a probability $\frac{\beta^2}{\alpha^2+\beta^2}$ being measured in |1> state:

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \alpha\begin{bmatrix}1\\ 0\end{bmatrix} + \beta\begin{bmatrix}0\\ 1\end{bmatrix}$$

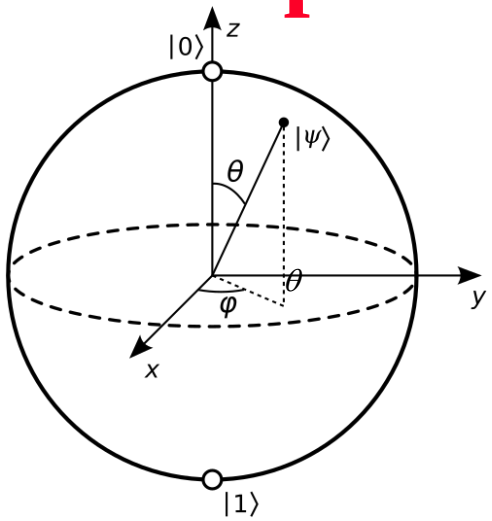
- This means that until it is measured, it is in both states.
- An electron can spin clockwise and counterclockwise at once.
- A photon can go through two slits simultaneously (as in the double-slit experiment).

This is called **superposition** (being in two places at once).

**Student Questions**


©2025 Raj Jain

# Bloch Sphere




- The north pole in this sphere represents |0> and the south pole represents |1>.
- All other points on the surface represent a superposition.
- $\theta$ is the angle from *z*-axis. Controls the balance between 0 and 1.
- $\phi$ is the angle around the equator (controls relative phase)
- All points on the equator have 50% probability of being measured as |0> and 50% probability of being measured as |1>.

**Student Questions**


©2025 Raj Jain

# Matrix Multiplication

- **Matrix multiplication ×:** Also called **dot product** A.B

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \end{bmatrix} \times \begin{bmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \\ b_{20} & b_{21} \end{bmatrix}$$

$$= \begin{bmatrix} a_{00}b_{00} + a_{01}b_{10} + a_{02}b_{20} & a_{00}b_{01} + a_{01}b_{11} + a_{02}b_{21} \\ a_{10}b_{00} + a_{11}b_{10} + a_{12}b_{20} & a_{10}b_{01} + a_{11}b_{11} + a_{12}b_{21} \end{bmatrix}$$

- Example:

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 0 & 0 & 0 \end{bmatrix}$$

**3×2** **2×3** **3×3**

**Student Questions**


©2025 Raj Jain

# Tensor Product

- **Tensor Product $\otimes$:** $m\times n \otimes k\times l$ results in $mk\times nl$ matrix

$$A=\begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} B=\begin{bmatrix} b_{00} & b_{01} & b_{02} \\ b_{10} & b_{11} & b_{12} \\ b_{20} & b_{21} & b_{22} \end{bmatrix}$$

$$A\otimes B=\begin{bmatrix} a_{00}\begin{bmatrix} b_{00} & b_{01} & b_{02} \\ b_{10} & b_{11} & b_{12} \\ b_{20} & b_{21} & b_{22} \end{bmatrix} & a_{01}\begin{bmatrix} b_{00} & b_{01} & b_{02} \\ b_{10} & b_{11} & b_{12} \\ b_{20} & b_{21} & b_{22} \end{bmatrix} \\ a_{10}\begin{bmatrix} b_{00} & b_{01} & b_{02} \\ b_{10} & b_{11} & b_{12} \\ b_{20} & b_{21} & b_{22} \end{bmatrix} & a_{11}\begin{bmatrix} b_{00} & b_{01} & b_{02} \\ b_{10} & b_{11} & b_{12} \\ b_{20} & b_{21} & b_{22} \end{bmatrix} \end{bmatrix}$$

$$=\begin{bmatrix} a_{00}b_{00} & a_{00}b_{01} & a_{00}b_{02} & a_{01}b_{00} & a_{01}b_{01} & a_{01}b_{02} \\ a_{00}b_{10} & a_{00}b_{11} & a_{00}b_{12} & a_{01}b_{10} & a_{01}b_{11} & a_{01}b_{12} \\ a_{00}b_{20} & a_{00}b_{21} & a_{00}b_{22} & a_{01}b_{20} & a_{01}b_{21} & a_{01}b_{22} \\ a_{10}b_{00} & a_{10}b_{01} & a_{10}b_{02} & a_{11}b_{00} & a_{11}b_{01} & a_{11}b_{02} \\ a_{10}b_{10} & a_{10}b_{11} & a_{10}b_{12} & a_{11}b_{10} & a_{11}b_{11} & a_{11}b_{12} \\ a_{10}b_{20} & a_{10}b_{21} & a_{10}b_{22} & a_{11}b_{20} & a_{11}b_{21} & a_{11}b_{22} \end{bmatrix}$$

## Student Questions


©2025 Raj Jain

# Tensor Product (Cont)

- Example 1:

$$\begin{bmatrix} a_{00} \\ a_{10} \\ a_{20} \end{bmatrix} \otimes \begin{bmatrix} b_{00} \\ b_{10} \end{bmatrix} = \begin{bmatrix} a_{00}\begin{bmatrix} b_{00} \\ b_{10} \end{bmatrix} \\ a_{10}\begin{bmatrix} b_{00} \\ b_{10} \end{bmatrix} \\ a_{20}\begin{bmatrix} b_{00} \\ b_{10} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_{00}b_{00} \\ a_{00}b_{10} \\ a_{10}b_{00} \\ a_{10}b_{10} \\ a_{20}b_{00} \\ a_{20}b_{10} \end{bmatrix}$$

**3×1** **2×1** **6×1**

- Example 2:

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

**2×2** **1×3** **2×6**

## Student Questions


©2025 Raj Jain

# Multiple Qubits and QuBytes

One Qbit: $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$

Two Qbits: $|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$ $|01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$ $|10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}$ $|11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$

Tensor Product

Three Qbits:

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

$|000\rangle$ $|001\rangle$ $|010\rangle$ $|011\rangle$ $|100\rangle$ $|101\rangle$ $|110\rangle$ $|111\rangle$

- In a *k*-qubit register, each of the $2^k$ positions can be any complex number
- QuByte=8-Qubits = 256-element vector

## Student Questions


©2025 Raj Jain

# Homework 16A

- Given two matrices:

$$A = \begin{bmatrix} 1+i & 1 \\ 1-i & i \end{bmatrix} B = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

- Compute: $A \times B,\ A \otimes B$

- Compute the probabilities of each element of $A \times B$

**Student Questions**


©2025 Raj Jain

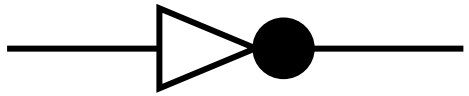
# Quantum Gates

1. Quantum NOT Gate
2. Quantum AND Gate
3. Quantum OR Gate
4. Quantum NAND Gate
5. Quantum √NOT Gate
6. Pauli Z-gate
7. Pauli X-gate
8. Pauli Y-gate
9. Hadamard H-Gate

**Student Questions**


©2025 Raj Jain

# Quantum NOT Gate

- **NOT:** 

Classical

| $x$ | $Not(x)$ |
|---|---|
| 0 | 1 |
| 1 | 0 |

Quantum

| $x$ | $Not(x)$ |
|---|---|
| $\|0>$ | $\|1>$ |
| $\|1>$ | $\|0>$ |

- All quantum gates are equivalent to matrix multiplication:

$$NOT = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} ? \\ ? \end{bmatrix}$$

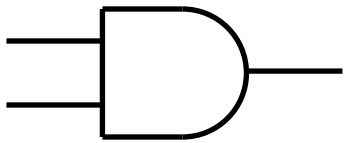
$$NOT\,|1> \;=\; |0> \qquad NOT\,|0> \;=\; |?>$$

**Student Questions**


©2025 Raj Jain

# Quantum AND Gate

- **AND:**



$$\text{AND}=\begin{bmatrix}1 & 1 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$$

| Classical | | | Quantum | |
|---|---|---|---|---|
| $x$ | $y$ | $x$^y | $xy$ | $x$^y |
| 0 | 0 | 0 | $\|00>$ | $\|0>$ |
| 0 | 1 | 0 | $\|01>$ | $\|0>$ |
| 1 | 0 | 0 | $\|10>$ | $\|0>$ |
| 1 | 1 | 1 | $\|11>$ | $\|1>$ |

- **Verify that:**

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

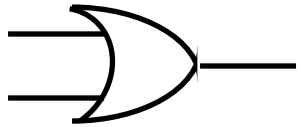
AND $|11>=|1>$

## Student Questions


©2025 Raj Jain

# Quantum OR Gate

- **OR:**



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

Classical

| $x$ | $y$ | $x \vee y$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |

Quantum

| $x, y$ | $x \vee y$ |
|---|---|
| $\|00>$ | $\|0>$ |
| $\|01>$ | $\|1>$ |
| $\|10>$ | $\|1>$ |
| $\|11>$ | $\|1>$ |

- **Verify that:**

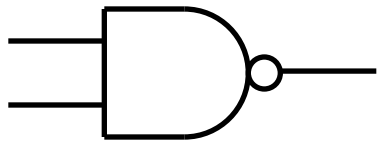
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

OR $|01>=|1>$

## Student Questions


©2025 Raj Jain

# Quantum NAND Gate

- **NAND:** 

$$\text{NAND} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

Classical

| $x$ | $y$ | $\overline{xy}$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Quantum

| $x, y$ | $x \wedge y$ |
|---|---|
| $\|00>$ | $\|1>$ |
| $\|01>$ | $\|1>$ |
| $\|10>$ | $\|1>$ |
| $\|11>$ | $\|0>$ |

Matrix Method

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

NAND $|00> = |1>$

- NAND gate is functionally complete in the sense that all other classical gates can be created using NAND, e.g.,
NOT(P)=NAND(P, P), AND(P, Q)=NAND(NAND(P,Q), NAND(P,Q))

**Student Questions**


©2025 Raj Jain

# Quantum √NOT Gate

- **√NOT:** √NOT ×√NOT = NOT

$$\sqrt{\text{NOT}} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$$

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} -1 \\ 1 \end{bmatrix} = |->$$

$|1>$

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = |+>$$

$|0>$

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \times \frac{1}{\sqrt{2}}\begin{bmatrix} -1 \\ 1 \end{bmatrix} = \begin{bmatrix} -1 \\ 0 \end{bmatrix} = - \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0>$$

$|0>$

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \times \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1>$$

$|1>$

## Student Questions

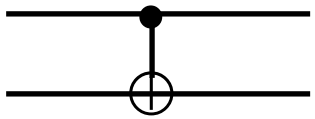

©2025 Raj Jain

# Controlled NOT Gate

- **CNOT:** If the control bit is 0, no change to the 2nd bit
  If control bit is 1, the 2nd bit is complemented

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

| $x, y$ | $CNOT(x, y)$ |
|---|---|
| $\|00>$ | $\|00>$ |
| $\|01>$ | $\|01>$ |
| $\|10>$ | $\|11>$ |
| $\|11>$ | $\|10>$ |



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

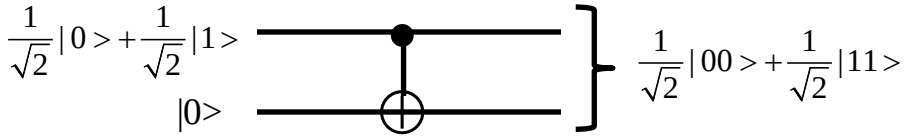
$$\text{CNOT} \quad |00> \quad |01> \quad |10> \quad |11> = |00> \quad |01> \quad |11> \quad |10>$$

- CNOT gate is invertible. It is its own inverse. That is, CNOT(CNOT($x$, $y$)) = ($x$, $y$)

**Student Questions**


©2025 Raj Jain

# Controlled NOT Gate (Cont)




- Controlled NOT gate can be used to produce two bits that are **entangled** ⇒ Two bits behave similarly even if far apart
  ⇒ Can be used for **teleportation** of information

**Student Questions**


©2025 Raj Jain



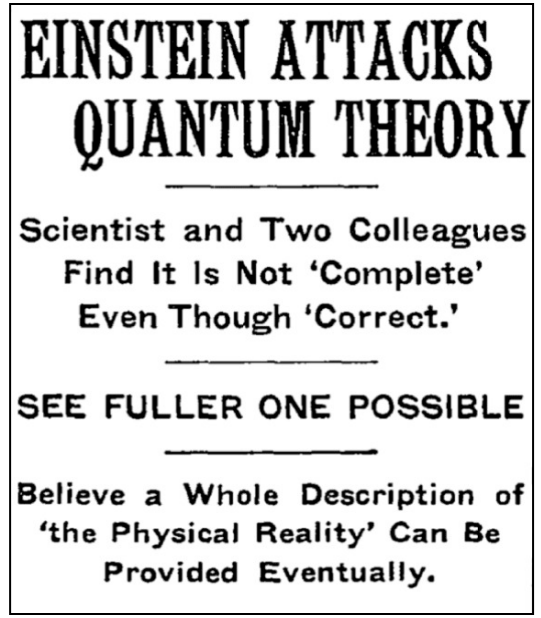
# Entanglement



Both think the same

- Two qubits can be entangled ⇒ Their states are correlated
  - Momentum, spin, polarization, or position are correlated
  - Even when they are far apart
  - Any change of one qubit affects the other
    ⇒ Teleportation of state ⇒ Quantum Key Distribution
- 1935: Einstein called it a paradox since change happens at speed faster than light
- 1967: Kocher developed an apparatus to produce entangled photons
- 1984: Quantum Key Distribution (QKD) protocols using entanglement
- 2022: Physics Nobel Prize for experiments with entangled photons

## Student Questions



EINSTEIN ATTACKS QUANTUM THEORY

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

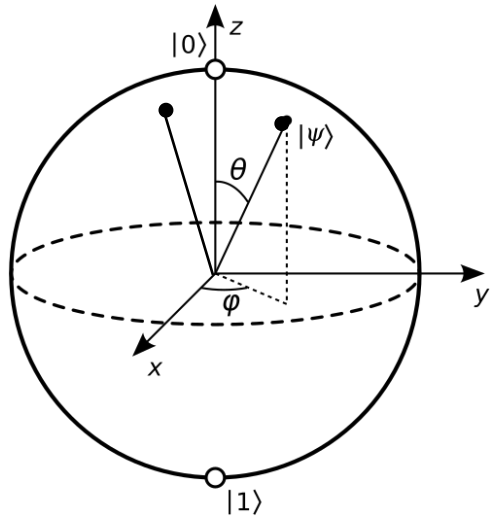
SEE FULLER ONE POSSIBLE

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

May 4, 1935 Issue of the New York Times, Source: Wikipedia


©2025 Raj Jain

# Pauli Z-Gate




- Acts on a single qubit. It flips the phase of a qubit's state by rotating it 180º around the z-axis of the Bloch Sphere

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

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \times \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix}$$

Z |0> = |0> Z |1> = -|1> Z $|\psi> = -|\psi>$

- It is a phase-flip gate.
- Used in error correction, quantum fourier transfm, and controlled operations

## Student Questions

- How does a phase flip differ from a bit flip?

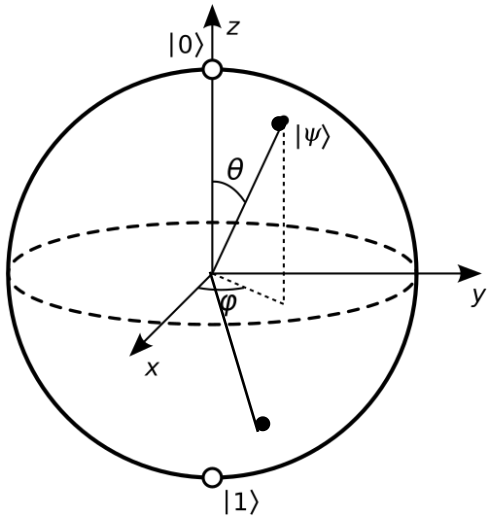
Phase Flip: $\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \rightarrow \begin{bmatrix} \alpha \\ -\beta \end{bmatrix}$

Bit Flip: $\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \rightarrow \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$


©2025 Raj Jain

# Pauli X-Gate

- Acts on a single qubit. It performs a bit-flip operation by rotating the qubit 180º around the *x*-axis of the Bloch Sphere




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

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

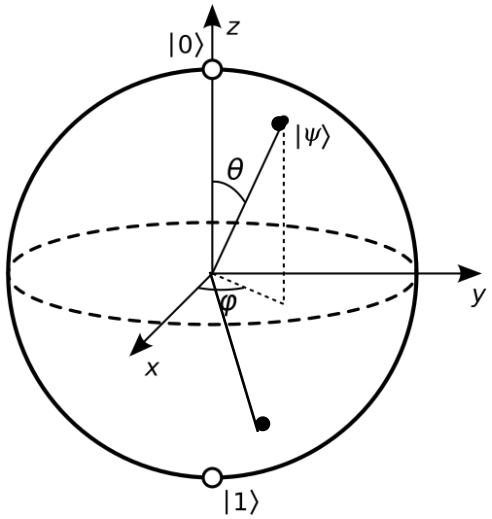
X |0> = |1> X |1> = |0> X $|\psi>$

- It is a bit-flip gate.
- Used in error correction to reverse bit-flip errors.

**Student Questions**


©2025 Raj Jain

# Y-Gate




- Acts on a single qubit. It performs a combined bit-flip and phase-flip operation by rotating the qubit 180º around the y-axis of the Bloch Sphere

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -i \\ 0 \end{bmatrix} = -i \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Y |1> = |0>

$$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix} = i \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \qquad \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \times \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} -i\beta \\ i\alpha \end{bmatrix} = \begin{bmatrix} -\beta \\ \alpha \end{bmatrix} = \begin{bmatrix} \beta \\ -\alpha \end{bmatrix}$$

Y |0> = |1> Y $|\psi>$

- It is a bit-flip and phase-flip gate.
- Used in creating entanglements and interference.

**Student Questions**


©2025 Raj Jain

# Hadamard Gate

- **Hadamard gate (H-gate)** creates quantum **superposition** by transforming a qubit from a definite state into an equal mixture of both. Performs a $\pi$ rotation around the z-axis followed by $\pi/2$ rotation around the y-axis.

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

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}\left\{\begin{bmatrix} 1 \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right\}$$

$$\text{H} \quad |1\rangle \quad = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$$

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\left\{\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right\}$$

$$\text{H} \quad |0\rangle \quad = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$$

- Superposition allows quantum parallelism – allowing a single qubit to explore multiple states simultaneously.

**Student Questions**


©2025 Raj Jain

# Quantum Gates: Summary

$$\text{NOT}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \qquad \text{AND}=\begin{bmatrix}1 & 1 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$$

$$\text{OR}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 1 & 1\end{bmatrix} \qquad \text{NAND}=\begin{bmatrix}0 & 0 & 0 & 1\\ 1 & 1 & 1 & 0\end{bmatrix}$$

Classical

$$\sqrt{\text{NOT}}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix} \qquad \text{CNOT}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

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

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

$$\text{T}=\begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\end{bmatrix}$$

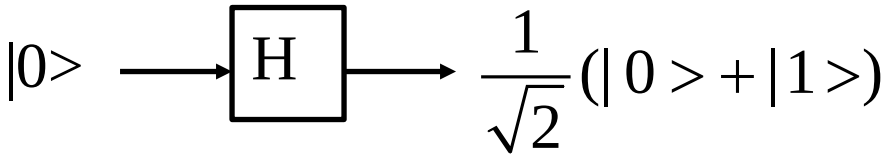
Non-Classical

## Student Questions


©2025 Raj Jain

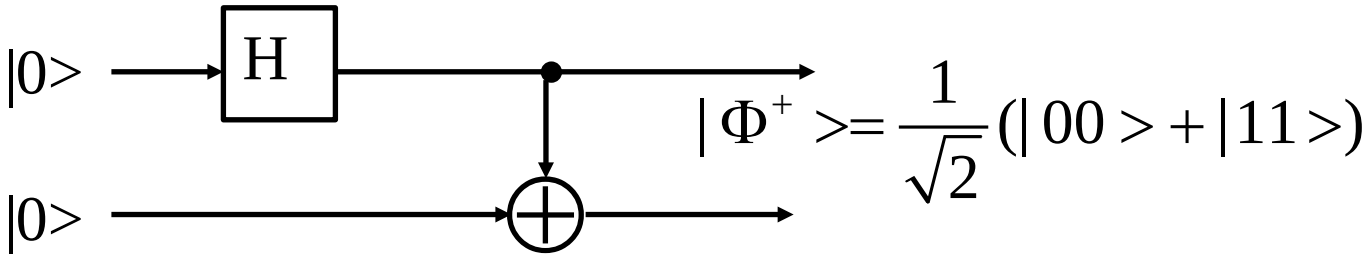
# Quantum Circuits

- A single-qubit example:




The output is a superposition of basis states |0> and |1>.

- A two-qubit example with two gates:




- This is called the **Bell State Circuit**. It takes two qubits in state |00>, applies a Hadamard gate, applies its output to a CNOT gate as a control for the 2nd qubit. Creates two **entangled bits**.

## Student Questions

- Why can quantum computation perform tasks like Fourier transforms and factoring large numbers more efficiently than classical computers?

*Requires further classes in quantum circuits. CSE quantum course covers it in detail.*


©2025 Raj Jain

# Impact of Quantum Computing on Security

- Current Security Methods are largely based on RSA, which is based on the difficulty of factorization of large numbers
- As the computers become faster, we keep increasing the key size: RSA-1024, RSA-2048, …
- **Quantum Threat**: Peter Shor showed in 1994 that quantum computers can factorize numbers exponentially faster than legacy computers.

Adopt quantum-safe security.

**Student Questions**


©2025 Raj Jain

# Post-Quantum Cryptography

- The National Institute of Standards and Technology (NIST) has finalized:
  - **FIPS 203: ML-KEM**: Based on CRYSTALS-Kyber (lattice-based) replaces RSA and ECC for secure key distribution.
  - **FIPS 204: ML-DSA**: Based on CRYSTALS-Dilithium and FALCON (also lattice-based) for digital signatures.
  - **FIPS 205: SLH-DSA**: Based pm SPHINCS+ for hash-based signatures. For long-term integrity in archival and regulatory environments
- Hardware vendors have incorporated quantum-resistant algorithms in Trusted Platform Modules (TPMs), Hardware Security Modules (HSMs)

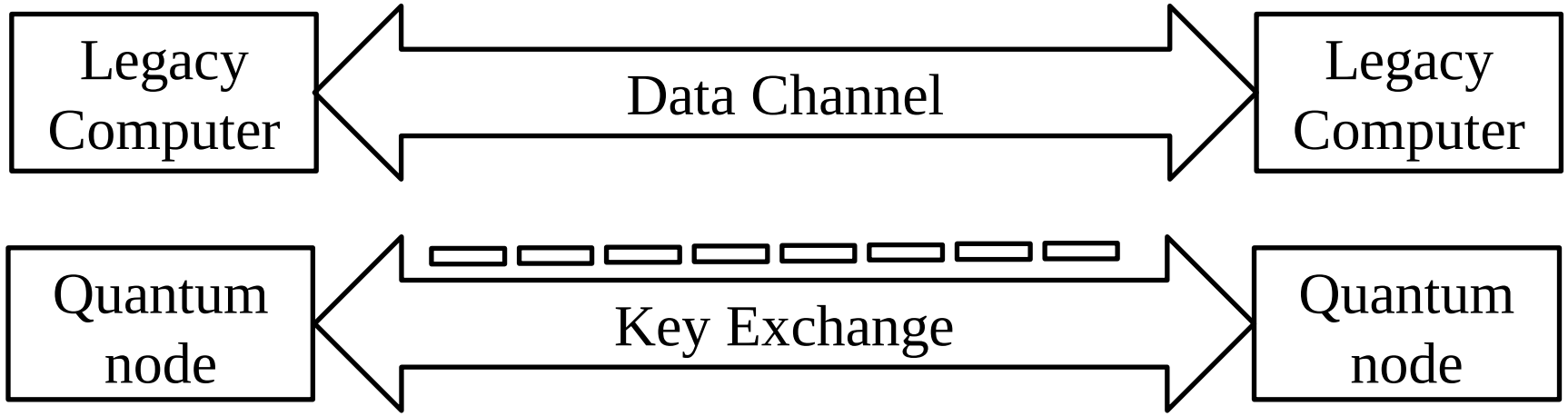
**Ref**: Post-Quantum Cryptography Coalition, https://pqcc.org


©2025 Raj Jain

**Student Questions**

# Quantum Key Distribution (QKD)

- Quantum computers are not yet suitable for very high-speed data transfer
- One important property of quantum bits (qubits) is that if you read it, it is destroyed ⇒ If anyone on the way reads a qubit, the receiver will know
- Quantum Link is a secure way to transfer encryption keys.
- While data goes on the traditional networks




**Student Questions**

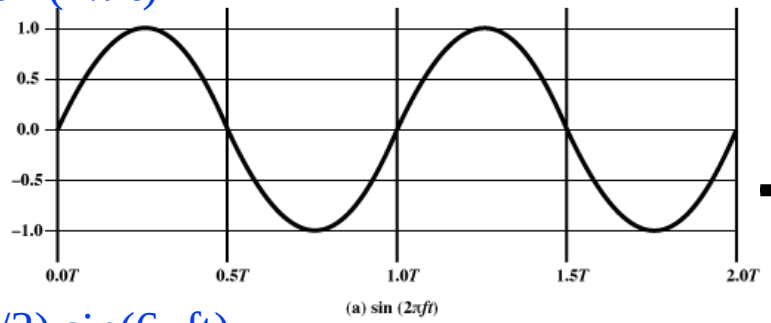

©2025 Raj Jain

# Fourier Transforms

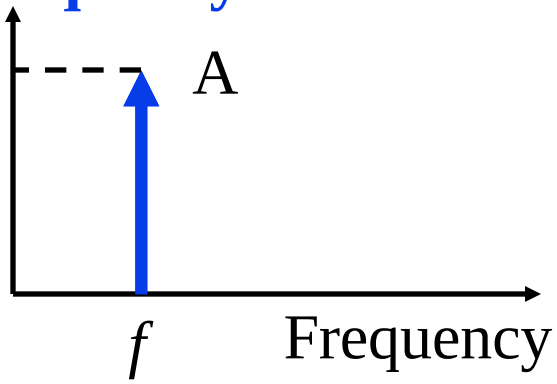
## Time Domain

## Frequency Domain

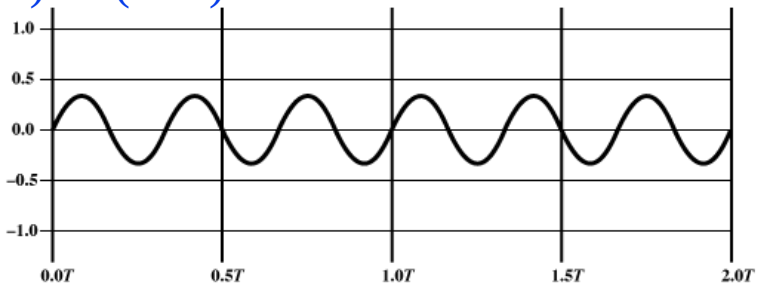
A sin(2πft)

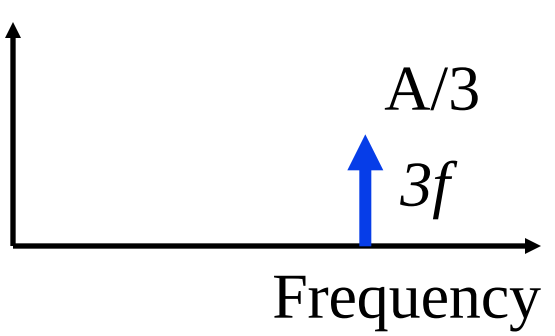



Fast Fourier Transform

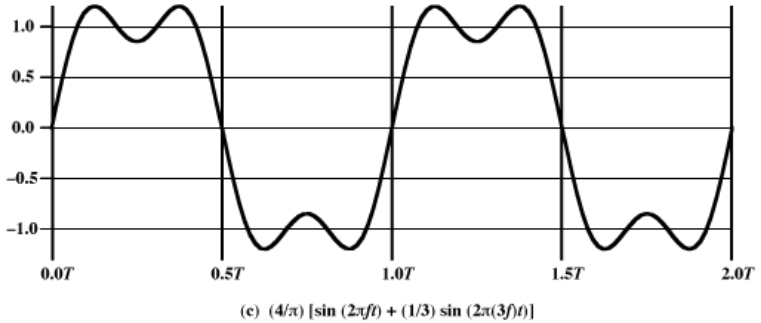


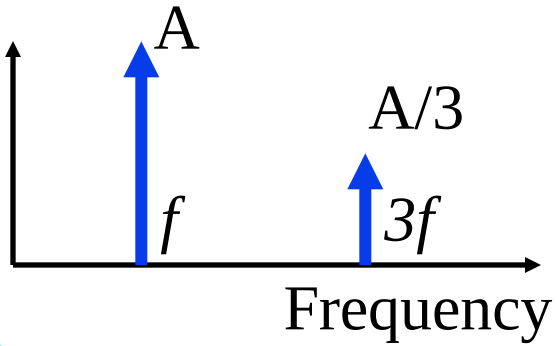

(A/3) sin(6πft)




A(Sin(2πft)+(1/3) sin(6πft))




## Student Questions



©2025 Raj Jain

# Quantum Fourier Transform (QFT)

- Fourier transform is used to find periodic components of signals
- QFT is faster than classical FT for large *inputs*

**Student Questions**


©2025 Raj Jain

# GCD

- Greatest Common Divisor of any two numbers
  - Divide the larger number with the smaller number and get the remainder less than the divisor
  - Divide the previous divisor with the remainder
  - Continue this until the remainder is zero.
    The last divisor is the GCD

```
15)  35   (2
     30
     ---
     05)  15   (3
          15
          --
           0
```

gcd

## Student Questions


©2025 Raj Jain

# Shor's Factoring Algorithm

- Peter Shor used QFT and showed that Quantum Computers can find prime factors of large numbers exponentially faster than conventional computers
- **Step 1:** Find the period of $a^i$ mod N sequence.
  Here $a$ is co-prime to $N \Rightarrow a$ is a prime such that gcd($a$, $N$) = 1 $\Rightarrow a$ and $N$ have no common factors.
  - Example: $N$=15, $a$=2;
    $2^i$ mod 15 for $i$=0, 1, 2, …
    = 1, 2, 4, 8, 1, … $\Rightarrow p$=4
  - If $p$ is odd, select another number.
    If mod($a^{p/2}$,$N$)=-1, select another number.
  - This is the classical method for finding periods.
    QFT makes it fast.
- **Step 2:** Prime factors of N might be $gcd(N, a^{p/2}+1)$ *and* $gcd(N, a^{p/2}-1)$
  - Example: $gcd(15, 2^2-1) = 3$; $gcd(15, 2^2+1) = 5$;

## Student Questions

- In Shor's Factoring Algorithm, the slide says that if the period p is odd, we should "select another number." Are we supposed to pick a different value of a? And why do these conditions make the algorithm fail?

*Yes, you should select a different a. If p is odd, $a^{p/2-1}$ is not an integer.*

# Homework 16B

- Find factors of 35 using Shor's algorithm, using $a$=3. Show all steps.
- Optional: Try factoring 407 (Answer: 11×37)

**Student Questions**


©2025 Raj Jain

# Quantum Machine Learning (QML)

- Quantum for solving systems of linear equation
- Quantum Principal Component Analysis
- Quantum Support Vector Machines (QSVM)
  - Classical SVM has runtime of O(poly($m$,$n$)), $m$ data points, $n$ features
  - QSVM has runtime of O(log($mn$))
    - Currently limited to data that can be represented with small number of qubits
- QML can process data directly from Quantum sensors with full range of quantum information

**Student Questions**

Ref: E. R. Johnston, N. Harrigan, and M. Gimeno-Segovia, "Programming Quantum Computers," O'reilly, 2019, ISBN:9781492039686, 320 pp.


©2025 Raj Jain

# Quantum Computing Technologies

1. **Superconducting Qubits**: Based on Josephson Tunnel junctions.
   - Strongly non-linear circuit elements at low temperature.
   - Unlike spins or atoms, they can be easily coupled to other circuits.
   - Used by Google, IBM, and Rigetti.
   - Pros: Fast gate times, scalable lithography
   - Cons: Requires cooling down to 10mK. Short coherence times.

Ref: Kjaergaard, Morten, et al. "Superconducting qubits: Current state of play." *Annual Review of Condensed Matter Physics* 11.1 (2020): 369-395, https://www.annualreviews.org/content/journals/10.1146/annurev-conmatphys-031119-050605?crawler=true&mimetype=application/pdf

**Student Questions**


©2025 Raj Jain

# Quantum Computing Tech (Cont)

2. **Trapped Ions:** Laser-controlled ions in electromagnetic traps.
   - Used by IonQ and Honeywell.
   - Pros: Long coherence, high fidelity.
   - Cons: Slow gates, Complex laser systems.
3. **Photonics**: Mirrors, beam splitters, and phase shifters are used to control photons.
   - Used by Xanadu, PsiQuantum.
   - Pros: Room temperature. Easy transmission.
   - Cons: Probabilistic gates, photon loss

**Student Questions**


©2025 Raj Jain

# Quantum Computing Technologies (Cont)

4. **Spin Qubits**: Electron or nuclear spins in semiconductor materials.
    4. Used by Intel, Delft University
    5. Pros: Long Coherence, CMOS compatibility
    6. Cons: Fabrication variability, control precision
5. **Neutral Atom**: A Group of cesium or rubidium atoms is cooled down to a few degrees Kelvin and controlled using lasers.
    4. Used by QuEra, ColdQuanta
    5. Pros: Reconfigurable arrays, long coherence
    6. Cons: Laser complexity, scaling control

**Student Questions**


©2025 Raj Jain

# Quantum Computing Technologies (Cont)

6. **Topological Quantum Computing**: Uses Anyons and Majorana zero modes
    6. Used by Microsoft
    7. Pros: Intrinsic error protection
    8. Cons: Theoretical stage. Not yet realized.

**Student Questions**


©2025 Raj Jain

# Quantum Computing Tech: Comparison

| Architecture | Gate Speed | Coherence | Scalability | Maturity |
|---|---|---|---|---|
| **Superconducting** | Fast | Medium | High | High |
| **Trapped Ions** | Slow | High | Medium | Medium |
| **Photonic** | Medium | High | High | Medium |
| **Spin Qubits** | Medium | High | Medium | Low |
| **Neutral Atoms** | Medium | High | High | Medium |
| **Topological** | Unknown | Theoretical | High | Low |

- **Issues:** Error correction, Modularity, Networking

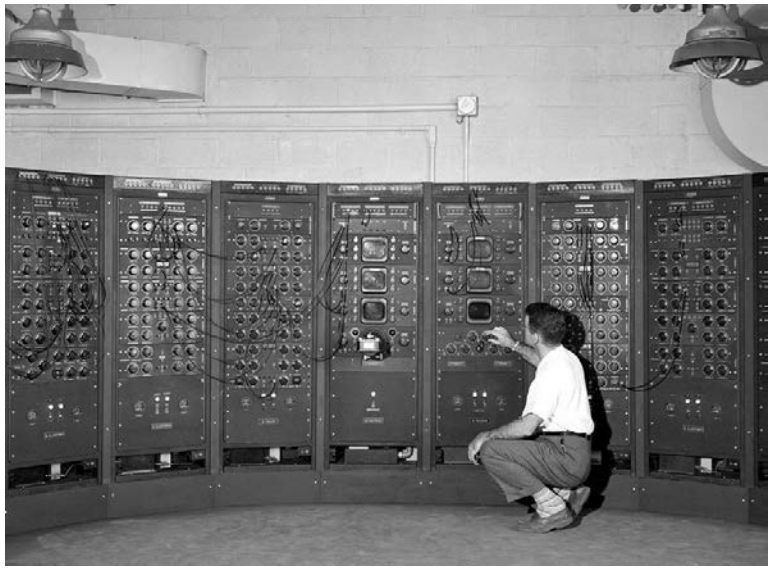
**Student Questions**


©2025 Raj Jain

# Quantum Hardware



IBM's Quantum computer



ENIAC (1943)

## Student Questions

Ref: https://www.zdnet.com/article/what-is-quantum-computing-everything-you-need-to-know-about-the-strange-world-of-quantum-computers/


©2025 Raj Jain

# Quantum Computing Applications

- **Optimization (Scheduling, Networking):** Logistics companies and Telcos are running quantum-assisted optimizers to reduce routing, scheduling, and resource-applications costs in real-time.
- **Approximate Optimization:**
  - Quantum approximate optimization algorithm (QAOA) using hybrid quantum-classical algorithms
  - Variational Quantum Eigen Solver (VQE) using hybrid quantum-classical algorithms. Used in quantum chemistry and material science since it is robust against noise. Ideal for the current **Noisy Intermediate-Scale Quantum** (**NISQ**).

**Student Questions**


©2025 Raj Jain

# Quantum Computing Applications (Cont)

- **Simulations for Autonomous Vehicle Testing**: Accelerated roading by simulating millions of scenarios related to weather, traffic, and terrain to test and validate.
- **Drug Discovery and Healthcare**: Simulating molecules to design new medicines
- **Materials Design and Chemistry**: Quantum simulations target catalysts, battery materials, and superconductors.
- **Finance**: Risk, portfolio optimization, derivative pricing with quantum optimizations
- **Artificial Intelligence**: Enhancing AI with hybrid quantum-classical models.

**Student Questions**


©2025 Raj Jain

# Quantum Computing Applications (Cont)

- **Cyberecurity**: Breaking traditional encryption and also developing quantum-proof security. Quantum key distribution.
- **Quantum Sensing**: Quantum sensors (atomic clocks, magnetometers, gravimeters) for navigation, geology, and fundamental physics experiments.
- **Climate Modeling**: Ultra-precise simulations of Earth's Climate
- **Space Research**: Helping Astrophysicists simulate dark matter, black holes, and cosmic events.

Ref: Forbes, "20 Real-world Applications of Quantum Computing to Watch," June 9, 2025, https://www.forbes.com/councils/forbestechcouncil/2025/06/09/20-real-world-applications-of-quantum-computing-to-watch/

**Student Questions**


©2025 Raj Jain

# Quantum Simulators

- QCEngine: https://oreilly-qc.github.io/
- Qiskit, https://qiskit.org/
  - Qiskit OpenQASM (Quantum Assembly Language), https://github.com/QISKit/openqasm/blob/master/examples/generic/adder.qasm
- Q# (Qsharp), https://docs.microsoft.com/en-gb/quantum/?view=qsharp-preview
- Cirq, https://arxiv.org/abs/1812.09167
- Forest, https://www.rigetti.com/forest
- List of QC Simulators, https://quantiki.org/wiki/list-qc-simulators
- See the complete list at: https://en.wikipedia.org/wiki/Quantum_programming

Ref: E. R. Johnston, N. Harrigan, and M. Gimeno-Segovia, "Programming Quantum Computers," O'reilly, 2019, ISBN:9781492039686, 320 pp.

**Student Questions**


©2025 Raj Jain

# Quantum Supremacy

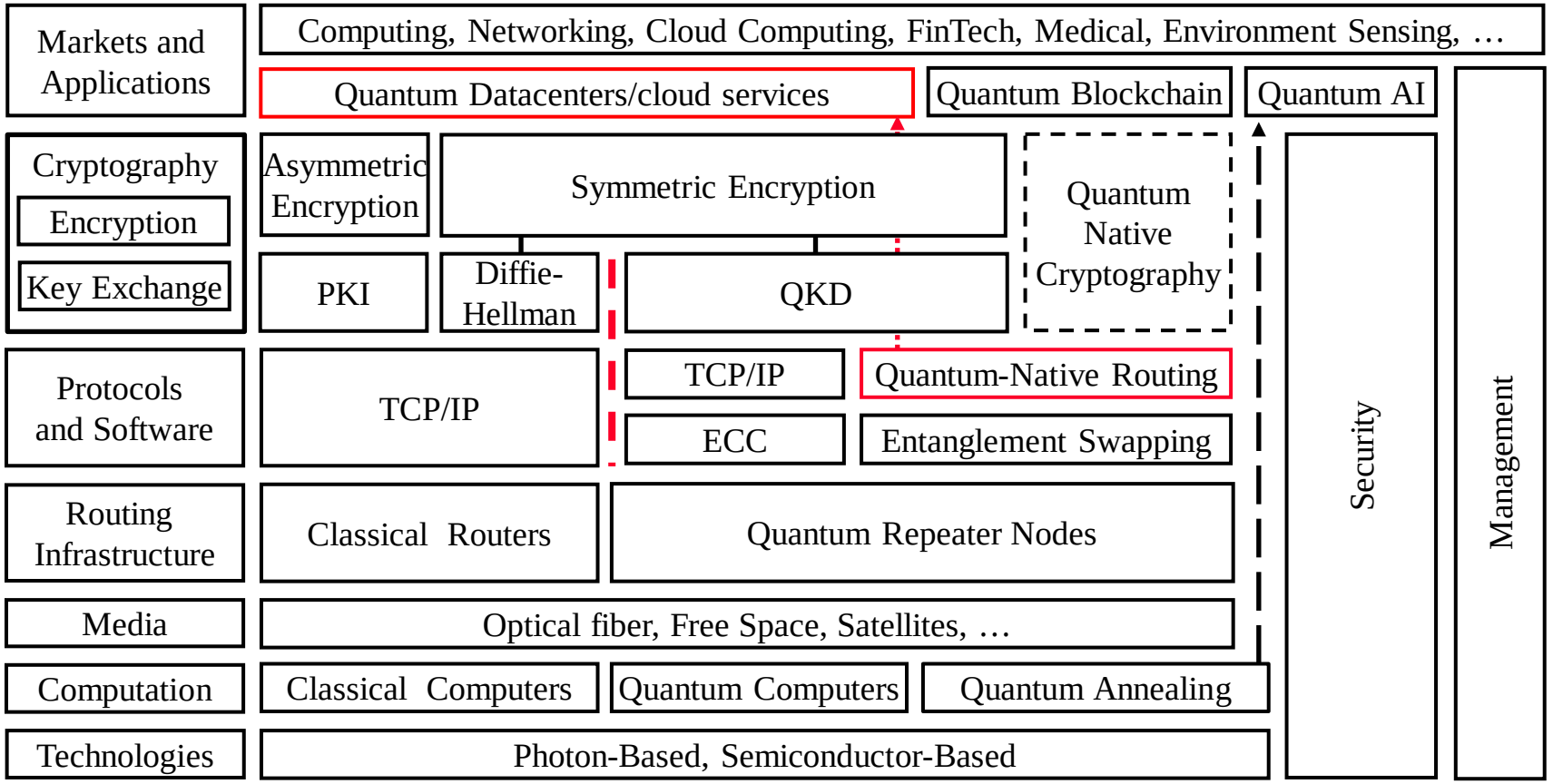
- Quantum Supremacy: Solve a problem on quantum computer that can not be solved on a classical computer
- Google announced it has achieved Quantum Supremacy on October 23, 2019
  - Google built a 54-qubit quantum computer using programmable superconducting processor
- Vendors: IBM, Microsoft, Google, Alibaba Cloud, D-Wave Systems, 1QBit, QC Ware, QinetiQ, Rigetti Computing, Zapata Computing
- Global Competition: China, Japan, USA, EU are also competing

**Student Questions**

Ref: F. Arute, K. Arya, R. Babbush, *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature* **574,** 505–510 (Oct. 23, 2019), https://www.nature.com/articles/s41586-019-1666-5


©2025 Raj Jain

# 7-Layers Stack of Quantum Research




## Student Questions


©2025 Raj Jain

# Protocol Stack of Quantum Internet

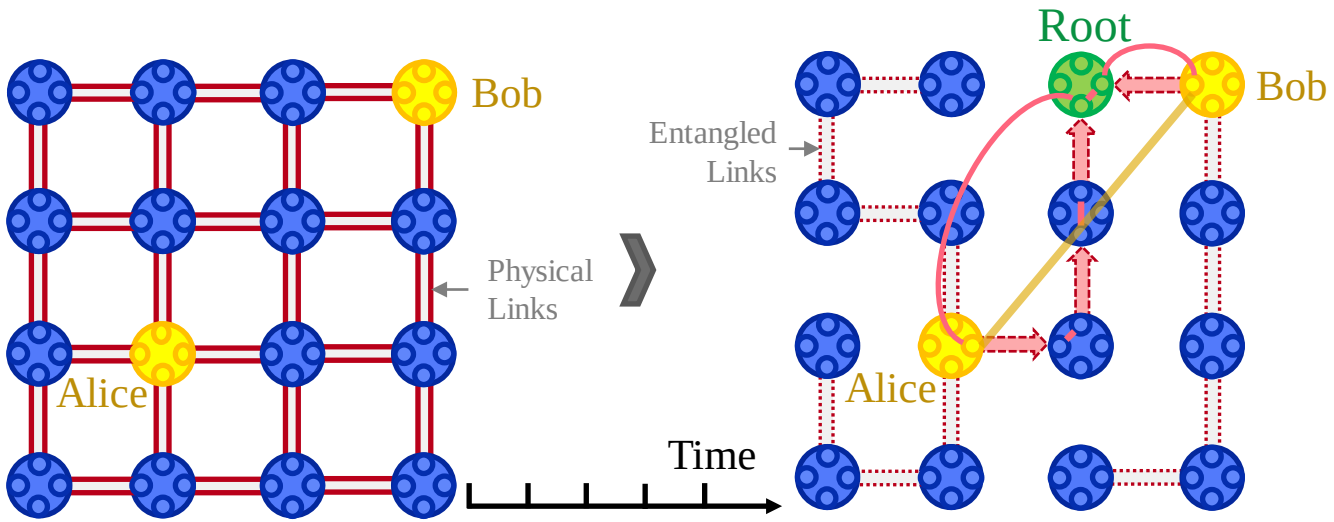
| Layers | Components | Example Technologies |
|---|---|---|
| *Application Layer* | Quantum cryptography | End-to-end QKD. |
| | Data transmission | Quantum teleportation. |
| | Large-scale computing | Distributed computing. |
| *Network Layer* | Quantum router | Routing protocols. |
| *Link Layer* | Quantum repeater scheme (direct-link protocol types) | Qubit forwarding.<br>Entanglement swapping.<br>QKD relay. |
| *Physical Layer* | Transmission medium (quantum channel and classical channel) | Optical fiber.<br>Free space/Satellite. |
| | Quantum computer | Photon-based.<br>Superconductor-based. |

**Student Questions**


©2025 Raj Jain

# Our Vision

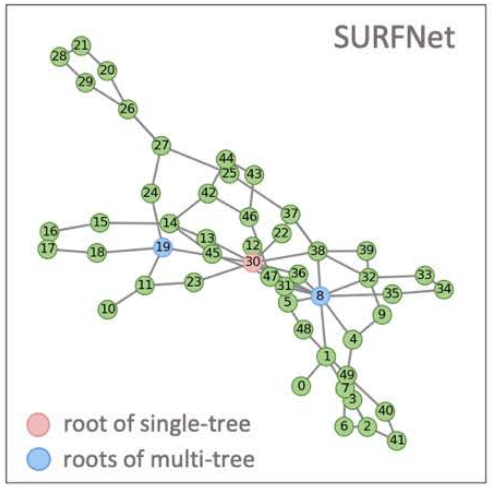
- We proposed an Asynchronous Entanglement Routing (**AER**) scheme using DODAG or a spanning tree, similar to those used in the Internet of Things and Ethernet.
- We completed the design, analysis, and simulation. Compared our results with the existing synchronous routing methods using the common grid topology:

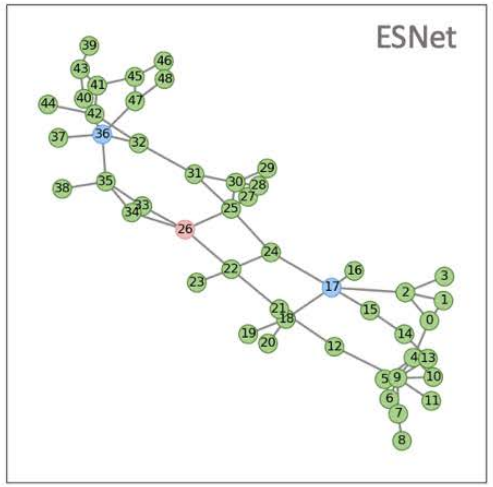


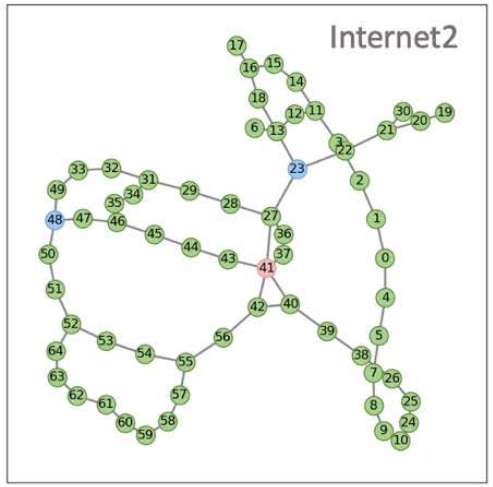

**Student Questions**


©2025 Raj Jain

# Realistic Topology Experiments



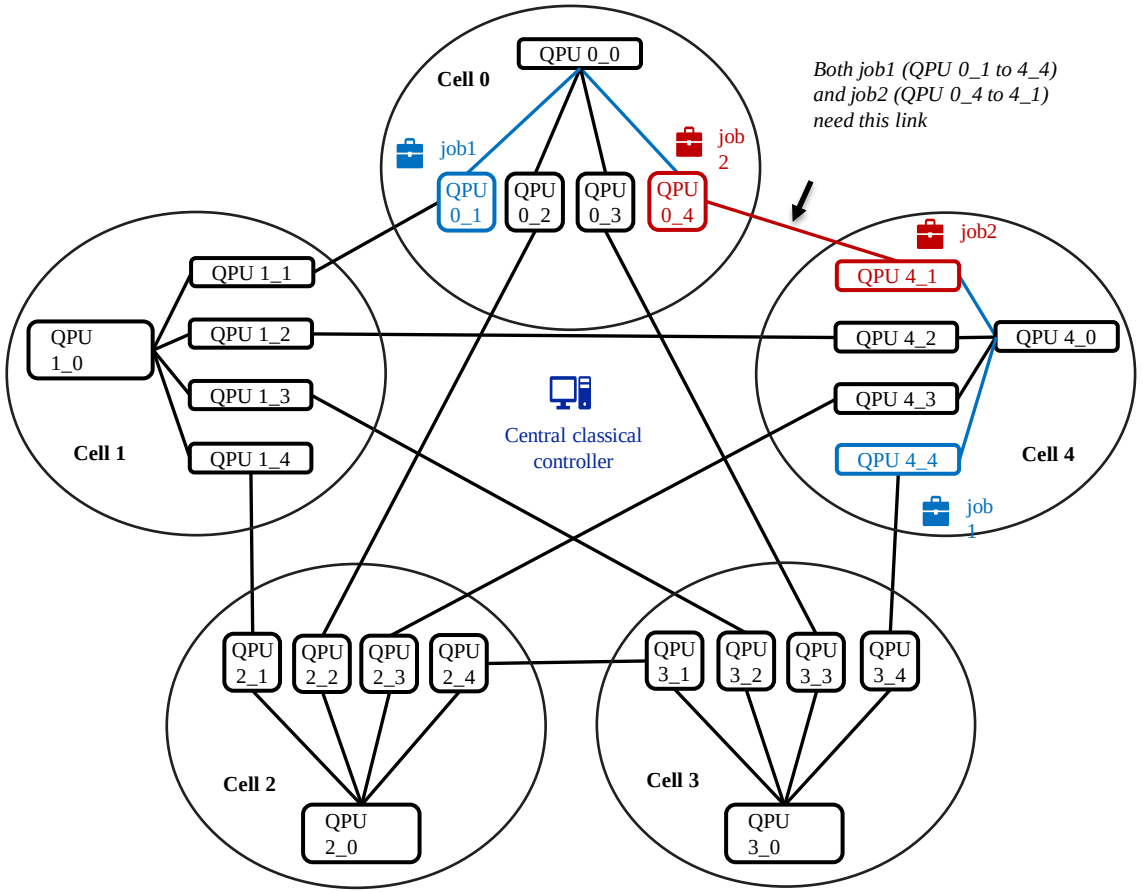

- The three topologies have different structures:

1. SURFNet has nodes with strong connections, as indicated by their higher number of adjacent edges, e.g., Node 8, making them suitable candidates for root nodes.
2. ESNet exhibits less densely distributed nodes and fewer highly connected central nodes than SURFNet.
3. Internet2 includes long linear chains in its topology.

## Student Questions

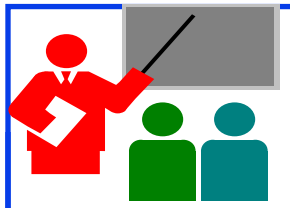
# Resource Management in Quantum Data Centers

- Consider an example data center with just 5 racks is shown here. Each rack is arranged as a cell (ellipse).
- The lines indicate quantum links created by entanglements. Each link may have multiple qubits entangled, and so have different capacities.
- Quantum jobs require a path between their source and destination QPU.
- If more than one job needs the same link, it has to be **fairly** and **efficiently** shared.




## Student Questions


©2025 Raj Jain



# Summary

1. A qubit is a two-element vector. Each element is a complex number that indicates the probability of that level
2. Multi-qubits are represented by tensor products of single-qubits
3. Qubit operations are mostly matrix operations. The number of possible operations is much larger than in classic computing.
4. Shor's factorization algorithm is an example of an algorithm that can be done in exponentially faster time than in classical computing.
5. Quantum computing is here. IBM, Microsoft, and Google all offer platforms for writing simple quantum computing programs and familiarizing yourself.
6. Quantum-Safe Crypto has been standardized.

**Student Questions**


©2025 Raj Jain

# Reading List

- C. Bernhardt, “Quantum Computing for Everyone,” The MIT Press, ISBN:9780262539531, 2019, 194 pp., Available online in WUSTL Library for WashU students. **Recommended.**
- Mercedes Gimeno-Segovia, Nic Harrigan, Eric R. Johnston, "Programming Quantum Computers," O'Reilly Media, Inc., July 2019, ISBN:9781492039686 (Safari Book). **Recommended.**
- FreeCodeCamp, “Quantum Computing Course – Math and Theory for Beginners,” YouTube Video, 1 Hr, 36 min, https://www.youtube.com/watch?v=tsbCSkvHhMo&pp=ygUOcXVhbnR1bSBjb3Vyc2U%3D **Recommended.**

## Student Questions


©2025 Raj Jain

# References


- Gerd Leuchs, Dagmar Bruss, "Quantum Information," 2 Volume Set, 2nd Edition, Wiley-VCH, June 2019, ISBN:9783527413539 (Safari Book).
- Vladimir Silva, "Practical Quantum Computing for Developers: Programming Quantum Rigs in the Cloud using Python, Quantum Assembly Language and IBM QExperience," Apress, December 2018, ISBN:9781484242186 (Safari Book).
- Mingsheng Ying, "Foundations of Quantum Programming," Morgan Kaufmann, March 2016, ISBN:9780128025468 (Safari Book).
- F.J. Duarte, "Quantum Optics for Engineers," CRC Press, November 2017, ISBN:9781351832618 (Safari Book).
- Quantum Algorithm Zoo, (Compiled list of Quantum algorithms), http://quantumalgorithmzoo.org/
- J. D. Hidary, "Quantum Computing: An Applied Approach," Springer, 2019, 380 pp.
- N. S. Yanofsky and M. A. Mannucci, "Quantum Computing for Computer Scientists," Cambridge, 2008, 380 pp.
- N. D. Mermin, "Quantum Computer Science: An Introduction," Cambridge, 2007, 220 pp.


## Student Questions



©2025 Raj Jain

# Wikipedia Links

- **https://en.wikipedia.org/wiki/Category:Quantum_computing**
- https://en.wikipedia.org/?title=Inner-product&redirect=no
- https://en.wikipedia.org/wiki/Bra%E2%80%93ket_notation
- https://en.wikipedia.org/wiki/Complex_number
- https://en.wikipedia.org/wiki/Controlled_NOT_gate
- https://en.wikipedia.org/wiki/Dot_product
- https://en.wikipedia.org/wiki/Fourier_transform
- https://en.wikipedia.org/wiki/Greatest_common_divisor
- https://en.wikipedia.org/wiki/List_of_quantum_processors
- https://en.wikipedia.org/wiki/Matrix_multiplication
- https://en.wikipedia.org/wiki/Polar_coordinate_system
- https://en.wikipedia.org/wiki/Quantum
- https://en.wikipedia.org/wiki/Quantum_algorithm
- https://en.wikipedia.org/wiki/Quantum_computing
- https://en.wikipedia.org/wiki/Quantum_entanglement
- https://en.wikipedia.org/wiki/Quantum_error_correction

## Student Questions


©2025 Raj Jain

# Wikipedia Links (Cont)

- https://en.wikipedia.org/wiki/Quantum_Fourier_transform
- https://en.wikipedia.org/wiki/Quantum_logic_gate
- https://en.wikipedia.org/wiki/Quantum_machine_learning
- https://en.wikipedia.org/wiki/Quantum_mechanics
- https://en.wikipedia.org/wiki/Quantum_simulator
- https://en.wikipedia.org/wiki/Quantum_supremacy
- https://en.wikipedia.org/wiki/Quantum_technology
- https://en.wikipedia.org/wiki/Quantum_teleportation
- https://en.wikipedia.org/wiki/Qubit
- https://en.wikipedia.org/wiki/Shor%27s_algorithm
- https://en.wikipedia.org/wiki/Superconducting_quantum_computing
- https://en.wikipedia.org/wiki/Sycamore_processor
- https://en.wikipedia.org/wiki/Tensor_product
- https://en.wikipedia.org/wiki/Timeline_of_quantum_computing
- https://en.wikipedia.org/wiki/Category:Quantum_gates

**Student Questions**


©2025 Raj Jain

# Classic Papers on Quantum Computing

- R. P. Feynman, "Simulating Physics with Computers," *International journal of theoretical physics* 21.6 (1982): 467-488, http://www.springerlink.com/index/t2x8115127841630.pdf
- D. E. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400.1818 (1985): 97-117, , https://royalsocietypublishing.org/doi/abs/10.1098/rspa.1985.0070
- D. E. Deutsch, "Quantum Computational Networks," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 425.1868 (1989), 73-90. , https://royalsocietypublishing.org/doi/pdf/10.1098/rspa.1989.0099 (subscribers only)
- P. W. Shor, "Algorithms for Quantum Computation: Discrete Log and Factoring," Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, IEEE, 1994, p. 124
- A. Barenco et al., "Elementary gates for quantum computation," Physical Review A, March 22, 1995, https://arxiv.org/pdf/quant-ph/9503016

**Student Questions**


©2025 Raj Jain

# Classic Papers (Cont)


- L. K. Grover, "A fast quantum mechanical algorithm for database search," Proceedings, STOC 1996, Philadelphia PA, USA, pp. 212-219, https://arxiv.org/pdf/quant-ph/9605043
- G. Brassard et al., "Quantum Counting," 1998, https://arxiv.org/pdf/quant-ph/9805082
- G. Brassard et al., "Quantum Amplitude Amplification and Estimation," 2000, https://arxiv.org/pdf/quant-ph/0005055
- S. Lloyd, "Quantum Algorithm for Solving Linear Systems of Equations," American Physical Society, APS March Meeting 2010, March 15-19,2010


**Student Questions**



©2025 Raj Jain

# Acronyms

- AER Asynchronous Entanglement Routing
- AFRL Air Force Research Lab
- AI Artificial Intelligence
- AND Quantum AND Gate
- APAC Asia-Pacific
- APS American Physical Society
- ARL Army Research Lab
- ARPA Advanced Research Project Agency
- CAS Chinese Academy of Sciences
- CCNOT Complement-Complement NOT
- CMOS Complementary Metal-Oxide Semiconductor
- CNOT Complement NOT
- CRYSTALS Cryptographic Suite for ALgebraic Lattices
- DC District of Columbia
- DOD Department of Defense
- DODAG Destination Oriented Directional Acyclic Graph

## Student Questions


©2025 Raj Jain

# Acronyms (Cont)

| | |
|---|---|
| DOE | Department of Energy |
| DSA | Digital Signature Algorithm |
| ECC | Elliptic Curve Cryptography |
| ESNet | Energy Science Network |
| EU | European Union |
| FALCON | Fast-Fourier Lattice-based Compact Signature over NTRU |
| FIPS | Federal Information Processing Standard |
| FT | Fourier Transform |
| GCD | Greatest Common Denominator |
| HSM | Hardware Security Modules |
| IARPA | Intelligence Advanced Research Project Agency |
| IBM | International Business Machines |
| IEEE | Institution of Electrical and Electronics Engineers |
| ISBN | International Standard Book Number |
| KEM | Key Encapsulation Mechanism |
| MIT | Massachusetts Institute of Technology |

## Student Questions


©2025 Raj Jain

# Acronyms (Cont)

| | |
|---|---|
| mK | Milli-Kelvin |
| ML | Machine Learning |
| MO | Missouri |
| NAND | Not of AND |
| NASA | National Aeronautics and Space Administration |
| NISQ | Noisy Intermediate-Scale Quantum |
| NIST | National Institute of Standards and Technology |
| NOT | Not |
| NQCO | Quantum Coordination Office |
| NQN | National Quantum Nanofab |
| NRDC | National Development Reform Council |
| NSA | National Security Agency |
| NSF | National Science Foundation |
| NTRU | Number Theory Research Unit |
| OpenQASM | Qiskit Open Quantum Assembly Language |
| OR | Or gate |

## Student Questions


©2025 Raj Jain

# Acronyms (Cont)

| | |
|---|---|
| PA | Pennsylvania |
| QAOA | Quantum approximate optimization algorithm |
| QC | Quantum Computing |
| QCEngine | Quantum Computing Engine |
| QExperience | Quantum Experience |
| QFT | Quantum Fourier Transform |
| QinetiQ | A security and defense contractor |
| QISKit | IBM's quantum simulation package |
| QKD | Quantum Key Distribution |
| QML | Quantum Machine Learning |
| QPU | Quantum Processing Unit |
| QSVM | Quantum Support Vector Machine |
| QuByte | Quantum Byte |
| QuEra | QuEra company |
| QUIET | A place to study quantum shielded from the effects of noise |
| RSA | Rivest, Shamir, Adleman |

## Student Questions


©2025 Raj Jain

# Acronyms (Cont)

- SDN — Software Defined Networking
- SLH-DSA — Stateless Digital Signature Algorithm
- SPHINCS — Practical stateless Hash-based Signature
- SURFNet — Samenwerkende Universitaire Rekenfaciliteiten (Cooperating University Computing) Facilities
- SVM — Support Vector Machine
- TPM — Trusted Platform Module
- UK — United Kingdom
- US — United States
- USA — United States of America
- USNO — United States Naval Observatory
- USTC — University of Science and Technology of China
- VQE — Variational Quantum Eigensolver
- WashU — Washington University
- WUSTL — Washington University in Saint Louis
- XOR — Exclusive OR gate

## Student Questions


©2025 Raj Jain

# Scan This to Download These Slides




Raj Jain
http://rajjain.com

http://www.cse.wustl.edu/~jain/cse5700-25/m_16qnt.htm

**Student Questions**


©2025 Raj Jain

# Related Modules



CSE567M: Computer Systems Analysis (Spring 2013),
https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n_1X0bWWNyZcof

CSE473S: Introduction to Computer Networks (Fall 2011),



https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcgy5e_10TiDw



Wireless and Mobile Networking (Spring 2016),
https://www.youtube.com/playlist?list=PLjGG94etKypKeb0nzyN9tSs_HCd5c4wXF

CSE571S: Network Security (Fall 2011),



https://www.youtube.com/playlist?list=PLjGG94etKypKvzfVtutHcPFJXumyyg93u



Video Podcasts of Prof. Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw

## Student Questions


©2025 Raj Jain