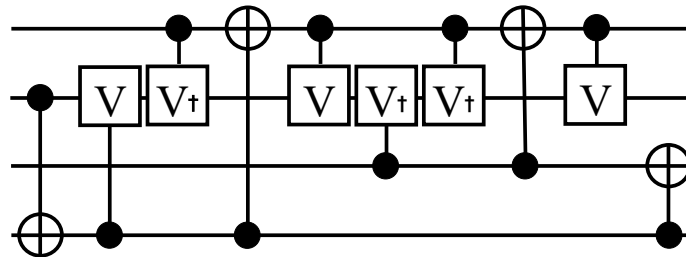


# ECE/CS 5/7384

## Introduction to Quantum Computing

Instructor: Mitch Thornton



GOAL: Introduction to the Ideas of  
Reversible and Quantum Logic and  
Computing

<https://s2.smu.edu/~mitch/class/5384/index.html>

1

## Class Grades

- **Homework/Labs** (25%) –Assigned periodically during the semester
- **Examination 1** (25%)- Test of the basic concepts between beginning of class and Mid-term
- **Examination 2** (25%)- Test of new concepts discussed in class to date of exam
- **Examination 3** (25%) – Final Exam

2

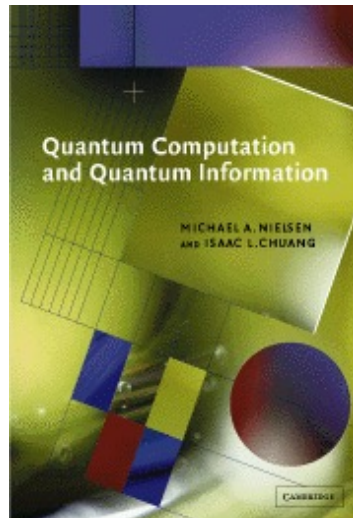
## Desired Student Background

- **Math** – linear algebra, discrete mathematics, elementary probability theory
- **Physics** – basic Physics courses required for undergraduate in the sciences/engineering, an introduction to quantum mechanical principles is desirable
- **CS/ECE** – computer architecture fundamentals, digital design fundamentals, exposure to algorithms and theory is desirable

Anyone with credit in the ECE 5/7383 Intro. to Quantum Informatics Automatically Satisfies the Desired Background

3

## Textbook



This is a comprehensive reference. We will not cover everything in this book.

4

## Other Material

- Main Textbook contains (*most of*) the general overview of the course material
- Selected Material from:
  - References
  - Historical Readings
  - Archived Papers
  - Other Web Resources
- Will ATTEMPT to place all notes online, BUT,
  - **YOU SHOULD TAKE NOTES ALSO**

5

## General Topic Outline

- Linear and selected topics from Tensor Algebra (review sessions online)
- Computation and the Laws of Physics (very brief)
- Relevant Concepts in Quantum Mechanics
- Hilbert Vector Spaces and the Notation of Dirac
- Quantum States and Measurement
- The Concept of the Qubit

6

## General Topic Outline (cont)

- The Bloch Sphere and Superposition
- Entanglement
- Reversible Logic
- Quantum Logic Gates
- No-Cloning Theorem
- Quantum Algorithms/Circuit Structure
- Survey of Known Algorithms

7

## Quantum Computing Overview

- New computing paradigm
- Certain algorithms show tremendous speedup
  - Overcomes limitations of Turing model
- Computes Fourier transform in  $O(\log n)^2$  rather than  $O(n \log n)$
- Database search in  $O(n^{1/2})$  rather than  $O(n)$  [Grover]
- Factorization in  $O(\log n)$  rather than  $O(n^{1/2})$  [Shor]

8

## Quantum Characteristics Exploited

- Quantum Superposition
- Entanglement
- Projective Measurement
- Information Teleportation
- Pure and mixed states
- No cloning theorem

9

## Quantum Bit (qubit)

- Superposition of basis (1 and 0) states:

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

where:

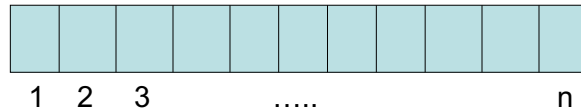
$$|\alpha|^2 + |\beta|^2 = 1 \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- Collapses into a basis state upon observation:

$$\text{Prob}(0) = |\alpha|^2 \quad \text{Prob}(1) = |\beta|^2$$

10

## Quantum Register/Computer\*



- Each cell contains a qubit
- Number of BASIS states is  $2^n$
- Gate Model of Computation (Deutsch'85):
  1. Initialize Qubits to known States (usually 0 basis state)
  2. Apply a sequence of Operations (called "gates")
  3. Read/Observe the final State of the Register

\*This is the Discrete Variable or "Gate-based" Model

11

## Qubit Basis States

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

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

## Some Single Qubit Quantum Gates

Hadamard

Pauli-X

Pauli-Y

Pauli-Z

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \mathbf{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

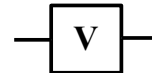
12

# Single Qubit Gates

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

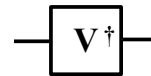
Square-root of X

$$V = \frac{1}{2} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}$$



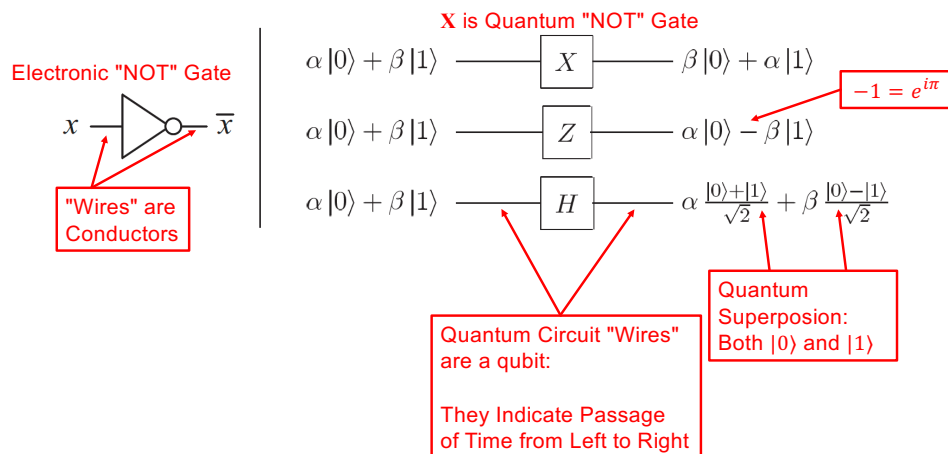
Square-root of  $X^\dagger$

$$V^\dagger = \frac{1}{2} \begin{bmatrix} 1-i & 1+i \\ 1+i & 1-i \end{bmatrix}$$



13

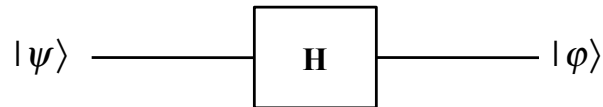
# Examples of Single Qubit Gates



14

## Example Computation

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



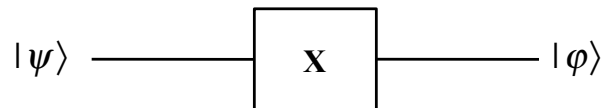
$$|\varphi\rangle = \mathbf{H}|\psi\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} \alpha + \beta \\ \alpha - \beta \end{bmatrix}$$

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

15

## Another Example Computation

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



$$|\varphi\rangle = \mathbf{X}|\psi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} = \beta|0\rangle + \alpha|1\rangle$$

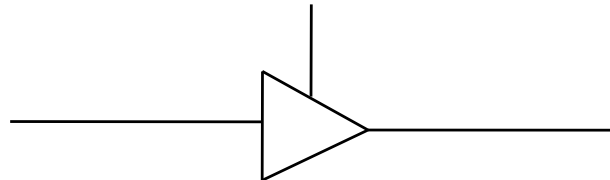
$$\mathbf{X}|0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle \quad \mathbf{X}|1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

16



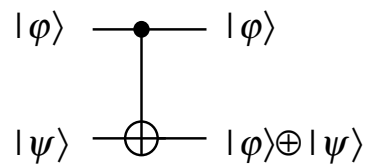
## Controlled Gates

- Allows State of one qubit to Control Transformation of Another
- Analogous to a “Control or Enable” Input on a Classical Electronic Logic Gate



17

## Controlled-X Gate



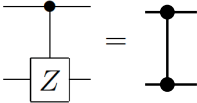



$$C_x = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Also, a “controlled-NOT” operator



18

## Two-qubit Gates

controlled-NOT		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
swap		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
controlled-Z		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
controlled-phase		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$




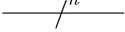
19

## Three-qubit Gates

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

20

## Other Quantum "Circuit" Symbols

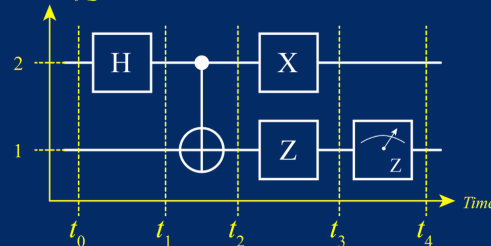
measurement		Projection onto $ 0\rangle$ and $ 1\rangle$
qubit		wire carrying a single qubit (time goes left to right)
classical bit		wire carrying a single classical bit
$n$ qubits		wire carrying $n$ qubits

21

## Quantum "Circuits"

- Accomplished with "Quantum Circuit" or with "Quantum Language"
- Quantum Circuits: Graphical Representations of Quantum Algorithms
  - Horizontal Lines are Qubit Instances that Evolve over Time
  - Operator Symbols Indicate a Transformation Applied at a Specific Time

Number of Qubits



OpenQASM\* Code Fragment:

```

h      psi;
CX     psi, phi;
x      psi;
z      phi;

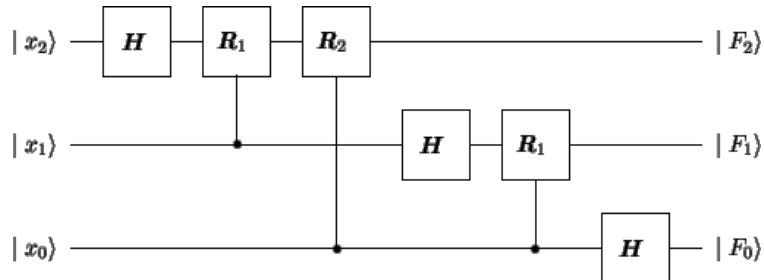
```

The term "Quantum Circuit," "Quantum Gates," and "Quantum Wires" can be Misleading!

These are Actually Quantum Algorithms!

22

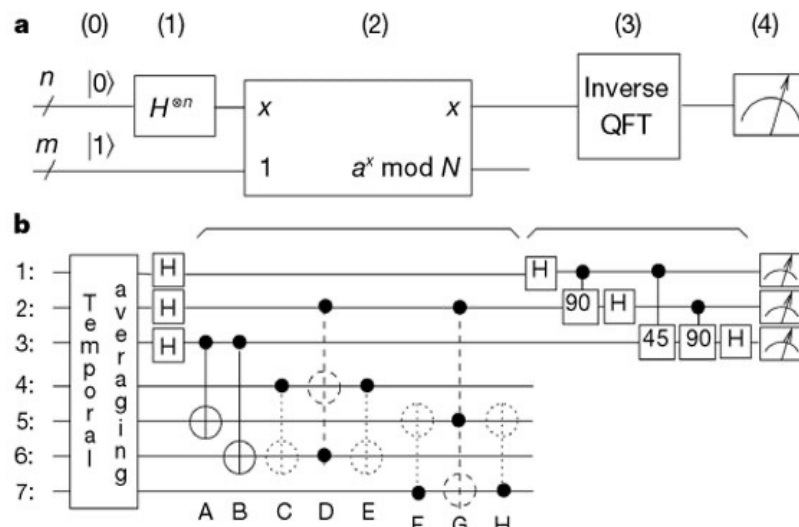
## Quantum Fourier Transform Circuit



6 gates suffice to compute an 8 component Discrete Fourier transform that would require 24 operations in FFT and 64 in straight DFT

23

## Shor's Algorithm



24

## Challenges in Quantum Computing

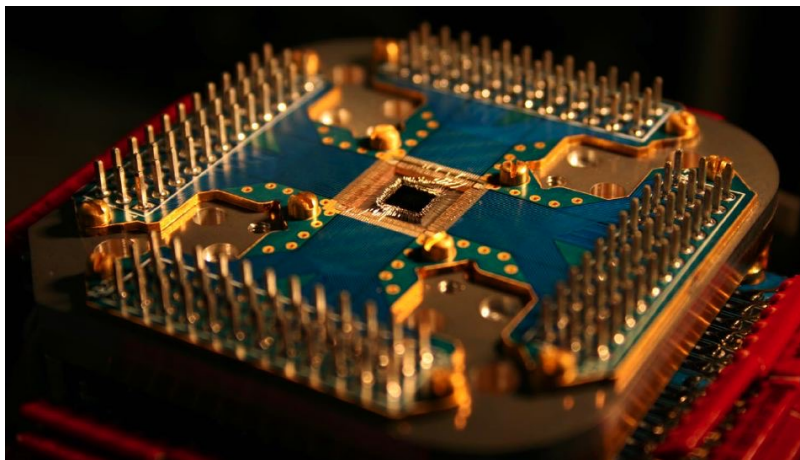
- Decoherence
- Error-correction
- Realizability of gates
- Initialization of the register
- Quantum Memory

25

## Current State of Quantum Computing

DWave - February 13, 2007

Is this Really a Quantum Processor?



source: <http://www.dwavesys.com/>

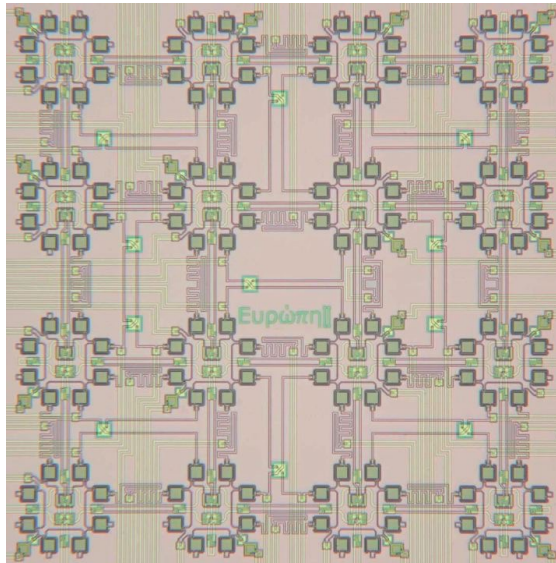
26

## D-Wave Technology Approach

- Based on Niobium metal loops with Josephson junctions
  - two superconductors separated by an insulator
- Tiny Loop currents exhibit quantum properties
  - direction of current flow represent “states” of qubit
  - eg. cw is “1”, ccw is “0”, both ways is superposition of “1” and “0”
- Based on theory of Adiabatic Computation rather than the gate model

27

## D-Wave 16-qubit Chip



source: <http://www.dwavesys.com/>

28

## Josephson Junctions

- Based on Current Flow across two weakly coupled superconductors
  - two superconductors separated by an insulator
- Current Crossing Insulator is “Josephson current”
- Quantum Mechanical effect known as “tunneling”
- Superconductors must be close to absolute zero degrees temperature

29

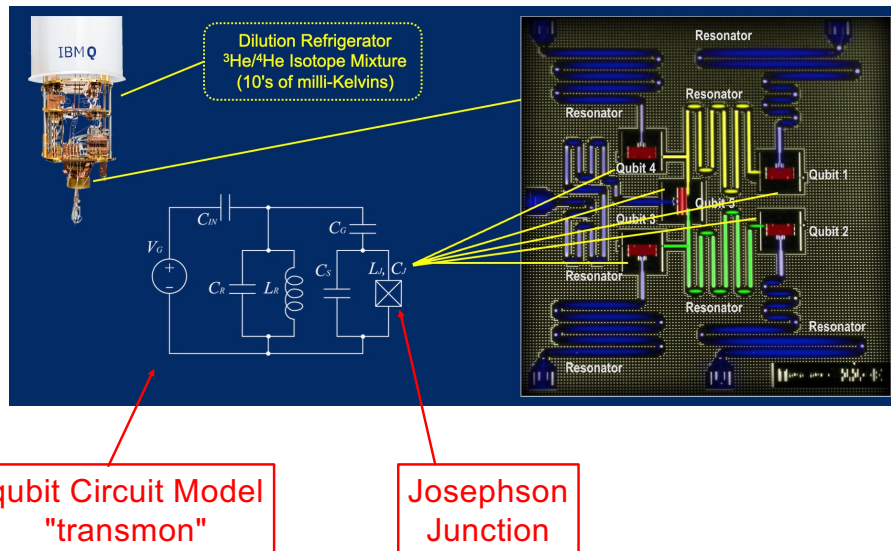
## D-Wave Cooling System



source: <http://www.dwavesys.com/>

30

## Early IBM QPU (5-qubit Yorktown)



31

## IEEE Spectrum January 2010

- Annual "Winners and Losers" Issue
  - Loser: D-Wave Does not Quantum Compute
- Experts Skeptical that D-Wave Computer is really a quantum computer
  - claims that "entanglement" has not been achieved
- D-Wave claims "making good progress"
  - currently testing three 128-qubit systems
- Consensus is that D-Wave has more work to do to demonstrate feasibility of approach

32



## IEEE Spectrum December 2012

- Quantum Computing “Proof of Concept”
- Implementation of Waveguides with Injected Bosons (Photons)
- Not Programmable – Hardware Solves One Proof of Concept Problem
- Conventional Machines can Compute Solution (for small number of bosons)
  - validation
- Uses Existing State-of-the-art Hardware
  - single photon generators, etc.

33

## Scientific American Dec./2014

- [“Quest for Quantum Computers Heats Up”](#)
- Google Hires Prof. Martinis Team
  - Univ. Santa Barbara Research Team
  - Extended Avg. Decoherence Time to minutes
  - Working with DWave
  - hiring “Quantum Engineers”
- IBM, Microsoft Active in Area
- Dutch QuTech Center using Quantum Dots
  - claim that there are “no more roadblocks”

34

## Where is the Technology Now?

- Two Main Competing Qubit Architectures
  - Ion Traps (IonQ, Quantinuum)
  - Josephson Junctions (Supercooled Semiconductors, IBM, Google, Rigetti)
  - Photons are Room-temp, but not as much Traction in the Technology Race
- The Race is on for:
  - More Qubits per QPU Chip
  - Logical (fault tolerant) Qubits to Prevent Decoherence

35

## Where is the Technology Now?

- IBM Condor (1,121 qubits)
- Atom Computing's system (1,180 qubits)
- D-Wave Advantage 2 (4,400 qubits)
- RIKEN & Fujitsu (256 qubits)
- NVidia ABCI-Q integrates QPU with GPU

36

## Cryptographically Significant Quantum Computer (CSQC)

- Shor's Algorithm Threatens PKI
  - quickly factors Semiprime Numbers that are Basis of Public-key Encryption Security
- Experts Believe tens to hundreds of thousand "physical qubits" Required and will be Available in the range of 5 to 30 years
  - NIST Standardized PQC Cryptographic Methods with First 3 (FIPS 203/204/205) Released in December 2024
- HNDL – "Harvest Now Decrypt Later" is Happening Right Now!