Under the Hood of the Quantum Computer

Bruce Harmon, PhD

Bruce.Harmon@du.edu

6 October 2021

Speaker

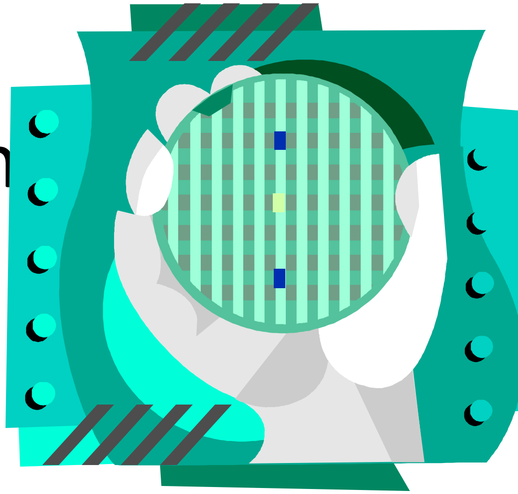
- Seventeen years with Hewlett Packard
  - Software/hardware/firmware/chip design, embedded systems design
  - Microprocessor and ASIC emulation R&D leadership
- Three with Synopsys, top EDA supplier
  - Tools for chip design
- Three more with Rudolph and KLA-Tencor, top suppliers in semiconductor wafer inspection
  - Rudolph for broadband visual macro inspection of individual die
  - K-T for UV-laser dark field inspection of wafers
- *University dean for computer science at Colorado Tech*
  - *Doctoral student did his dissertation on quantum computing*
- *Professor and program director for cybersecurity and data science at the University of Denver*
  - *Masters student doing independent research on quantum computing*

Outline of the Talk

- *Background and motivation of the talk*
- *What is quantum computing*
- *Quantum computing history*
- *Recent developments*
- *Quantum computing under the hood*
- *Implications to cyber security (cryptanalysis)*
- *Mitigation*

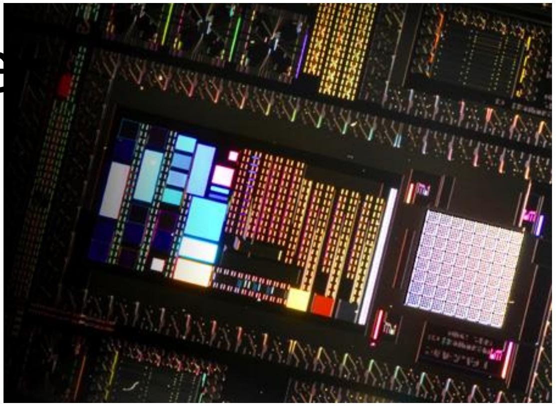
Background and Motivation

- A quantum computer, if it existed, would seriously threaten RSA encryption. This is via Peter Shor’s algorithm
- Research has been under way since 1980s
- Photon polarization and/or electron spin could enable
- Several companies claim to have on
- Hence the urgency



What's the Fuss: D-Wave, USC/LMC, NASA/Google

- 2011 D-Wave Systems made a chip-set and system: 128 qubit, to be homed at USC Lockheed Martin Quantum Computing Ctr
- Much criticized by academics; later published in *Nature*
- 2013 Google to form Quantum AI Lab at NASA Ames: 512 qubit sys from D-Wave



History of Quantum Computing

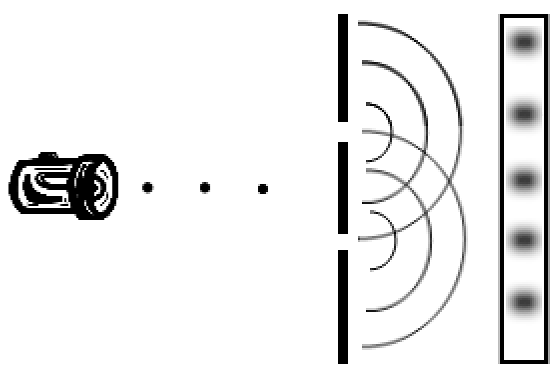
- Quantum mechanics since early 20^{th} Century: Einstein, Bohr, Planck, Dirac, Heisenberg, Schrodinger (remember the cat), et al
- One cannot know both the position and the momentum of a particle (Heisenberg)
- A photon can be in two places at once
- Digital computing since WW II era
- Quantum computing conceived in 1980s
  - Yuri Manin (1980), Richard Feynman (1982)
  - David Deutsch (1985)
  - Peter Shor (1994)

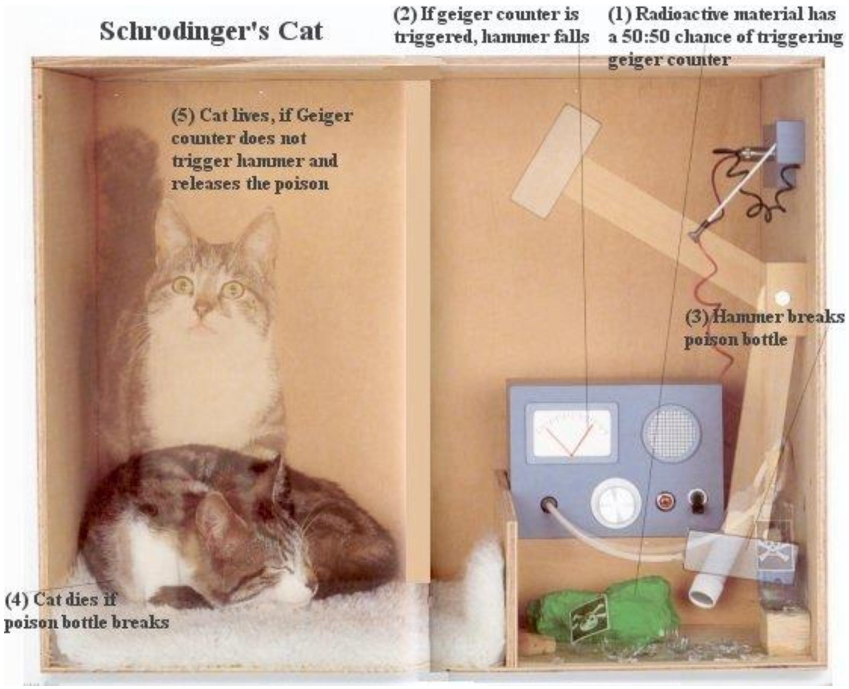
From Quantum Mechanics

- Discrete (from the latin *quanta*)
- “we cannot know the precise position and momentum of a quantum particle at the same time”
- Superposition
  - Heisenberg’s Principle (uncertainty)
    - Schrodinger’s cat, for example
  - One cannot know the state without testing
    - Thus invalidating or interfering
    - Results in a “collapse” to the measured state
- Entanglement: One knows only the aggregate; the individual properties are not known: “spooky action at a distance” -Einstein

Two-slit experiment; the cat

- Even single photon emission produces wave constructive and destructive interference
- Schrodinger’s cat is both alive and dead!?

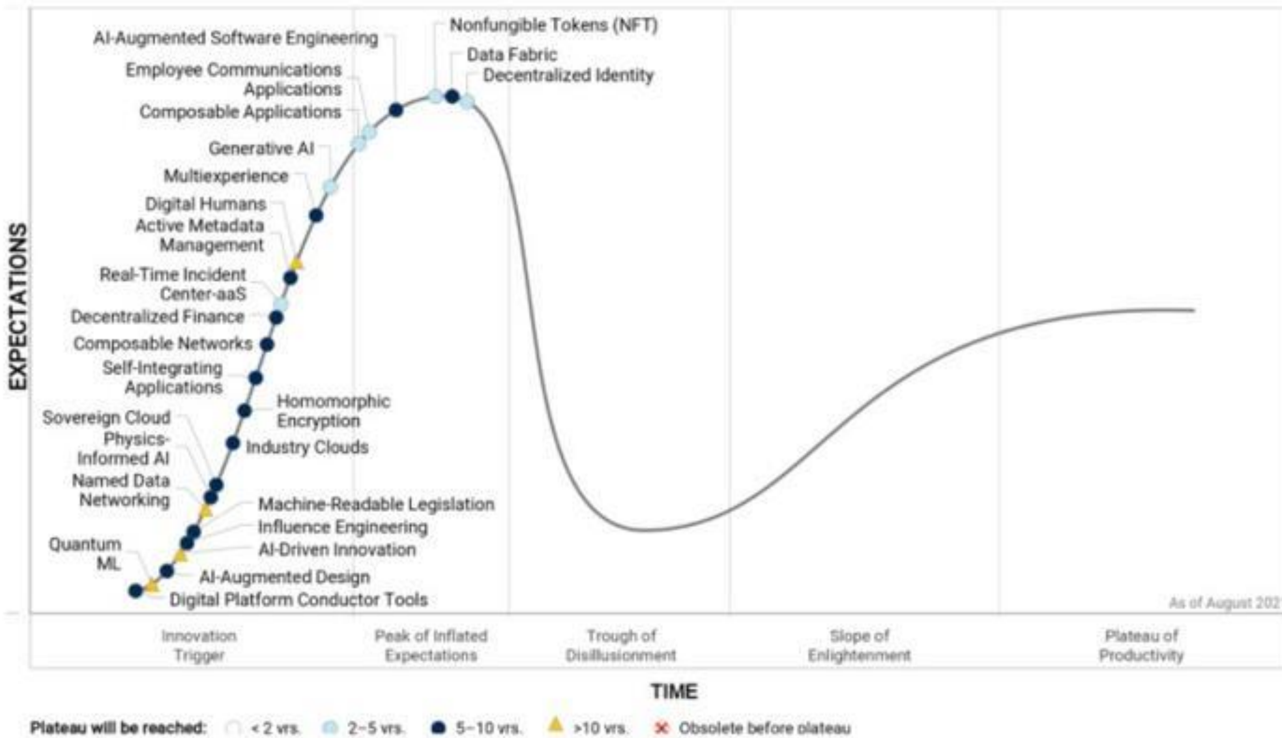




Applications

- Finding factors of large composite integers
- AI and machine learning
- Computational chemistry, biology
- Drug design
- Weather forecasting
- Optimization
- Financial modeling

QC makes it to the



Source: Gartner (August 2021)
747576

Source: Gartner (August 2021)

Quantum supremacy in 2019?

- Hello quantum world! Google publishes landmark quantum supremacy claim (nature.com)

Variations

- Quantum circuit model (most often used)
- Quantum Turing machine
- Adiabatic quantum computer
- One-way quantum computer

Exploitation

- If the details may be hidden by “entanglement”, *we may exploit that*
- In a manner similar to how the discrete (fast) Fourier Transform is able to exploit properties of the interplay between complex numbers and the periodicity of the exponential function
- Superposition
- The lack of detailed knowledge of the system may enable fast computation
- Measurement alters the system, and that can be exploited to detect eavesdropping

Under the hood

- Notation will be Dirac from Mermin
  - Cbit, Qbit, |0>, |1>, $|\phi >$
- Qbit is superposition as follows

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$$

  $|\alpha_0|^2 + |\alpha_1|^2 = 1$, α_i complex numbers
- One Qbit demands 2-vector space
- Two Qbit demands 4-vector space
- $|\alpha_0|^2$ is probability assoc. with |0>

Cbits are Qbits, too

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

Issues

- Noise
- Decoherence
  - Error correction
- Extreme cold required
- Multiple runs of the same program

Programming it

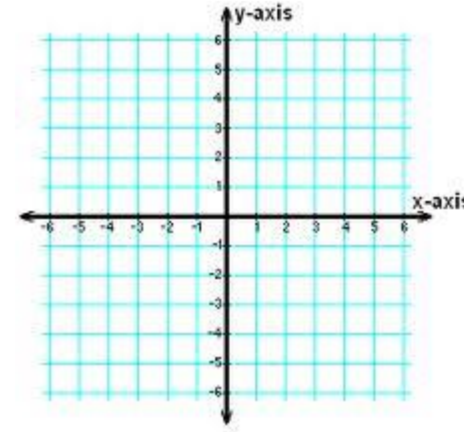
- List of QC simulators | Quantiki
- Quantum compiler with libraries
- C++, Python, Java, several others
- Simulate on a classical computer
- Assembly language metaphor
- Analogy to signal flow graphs or digital logic circuits
- Brilliant.com has a course in programming QC

QC programming is open source

- Cambridge Quantum makes TKET SDK open source (msn.com)

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

More on Qbits



- Computation basis (bases)
- |0> is $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, |1> is $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- We use orthonormal set of vectors for bases
- 2-Qbit uses 4-vector spaces

$$|\psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix}$$

- Generally one uses only 1 & 2-Qbits
- “A vector space of 2 or 4 dimensions over the complex numbers”

Architecture

- Input register of Qbits
- Output register of Qbits
- Logic in between is formed from Qbits
- Logic blocks are restricted to reversible, unitary transformations, designed to exploit properties
- Measurement blocks are irreversible and are used to get final answer only
- Final answer is a “collapse” based on probability

Clarifications

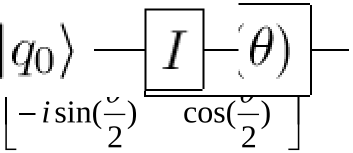
- Note matrix notation for transformations
- Reversible means the inputs can be determined by putting the outputs through the same transformation in reverse
- A unitary matrix as a transformation means that the inner product of the vector is preserved. The conjugate transpose equals the inverse.

Very brief review of linear algebra

- A square matrix can transform a column vector
  - y = A * x
- Such matrices can be cascaded
  - y = C * B * A * x
- Such a matrix is orthogonal if the L2 norm of each row and column is 1
- For example [[cos(theta), -sin(theta)],
  - [sin(theta), cos(theta)]] will rotate the vector by theta

Operators

- Exclusive OR
- Inner product
- Complex conjugation
- ***Linear, reversible, unitary transformations via matrices***
- Matrix multiplication



Common logic blocks

- **X,** NOT, negates, uses $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- $\boldsymbol{C_{i,j}}$**,** controlled NOT, if i==1 it negates, else no-op
- **S,** swap operator
- **Z,** uses $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- **H,** *Hadamard,* uses $\frac{1}{\sqrt{2}}(\boldsymbol{X} + \boldsymbol{Z})$
- **M,** measurement, not reversible

Single-qubit quantum gates

- Hadamard H = $\frac{1}{\sqrt{2}}\begin{vmatrix}1 & 1\\ 1 & -1\end{vmatrix}$
- Not X = $\begin{vmatrix}0 & 1\\ 1 & 0\end{vmatrix}$
- Z = $\begin{vmatrix}1 & 0\\ 0 & -1\end{vmatrix}$
- Identity I = HH = $\begin{vmatrix}1 & 0\\ 0 & 1\end{vmatrix}$

Methodology

- Input and output "kets" of qubits
- Signal flow diagrams
- 2^n = size of the alpha vector

Peter Shor's Algorithm

- Used to determine the period r associated with RSA, N=pq, b(x+r)=b(x)
- That, along with public key N, is enough to enable the tractable determination of the private key pq, which then breaks RSA
- Uses the quantum Fourier Transform, a quantum variant of the DFT/FFT
- Plus numerous number theory tricks
- Polynomial time vs. exponential time

Polynomial vs. exponential time

n	n^3	10^n
10	1000	1.00E+10
100	1.00E+06	1.00E+100
1000	1.00E+09	1E+1000
10000	1.00E+12	1E+10000

RSA

- Bob wants to receive from Alice; he knows N=pq and passes her only N and c; cd=1 mod (p-1)(q-1)
- Alice sends encoded msg b=a^c mod(N) which Bob can decode
  - a=b^d mod(N)
- Eve can only intercept and decode if she knows p or q

More Shor

- But if one could find the period r of the encoded msg b, one could directly decode b
- Roadmap: Use Shor to get r then use classical computer to find d to decode b

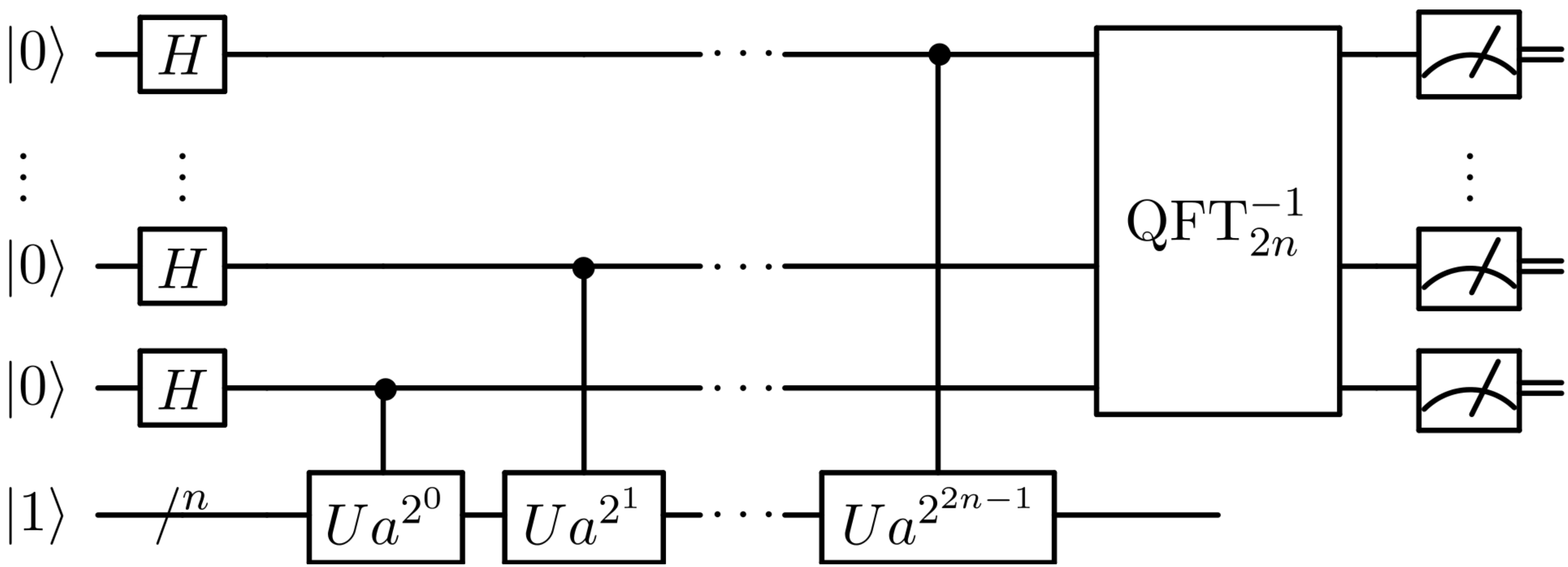
Quantum Fourier Transform

- $\boldsymbol{U}_{FT} = \boldsymbol{H}_3(\boldsymbol{V}_{32}\boldsymbol{H}_2)(\boldsymbol{V}_{31}\boldsymbol{V}_{21}\boldsymbol{H}_1)(\boldsymbol{V}_{30}\boldsymbol{V}_{20}\boldsymbol{V}_{10}\boldsymbol{H}_0)\boldsymbol{P}$
- Where **P** permutes the basis and
- $\boldsymbol{V}_{i,j} = \exp(i\pi\boldsymbol{n}_i\boldsymbol{n}_j/2^{|i-j|})$
- $\boldsymbol{n}_i$ is projection onto state *i*

More Shor

- $\boldsymbol{U}_{FT}$ is then applied to input register
- The output register is all we need from the quantum computer
- Number theory trick applied on conventional computer to get period r and then d
- Conventional computer then decodes b

Shor's



$|0\rangle$
$|0\rangle$
$|0\rangle$
$|1\rangle$
H
H
H
n
Ua^{2^0}
Ua^{2^1}
$Ua^{2^{2n-1}}$
QFT_{2n}^{-1}

Mermin on Shor’s

- Wayback Machine (archive.org)

D-Wave and IBM

- http://www.networkworld.com/news/2011/092611-quantum-computing-250825.html?source=NWWNLE_nlt_daily_am_2011-09-26
- IMHO: It is a good start but far from what would be needed for Shor’s
- http://www.networkworld.com/community/blog/ibm-scientists-discuss-quantum-computing-breakthrough?source=NWWNLE_nlt_daily_am_2012-02-28
- IBM’s Experimental Quantum Computing Lab approach described above

Mitigation?

- NIST is running a competition for it
- Post-Quantum Cryptography | CSRC (nist.gov)
- Post-Quantum Cryptography | CSRC (nist.gov)
- Quantum key distribution (QKD)
  - Polarized photons are used
- Post-quantum cryptography
- True randomness via quantum mechanics
- [2106.06640] Quantum-resistance in blockchain networks (arxiv.org)

References

- Mermin, N. David (2007). *Quantum Computer Science An Introduction.* Cambridge University Press.
- Purkeypile, M. D. (2009). *COVE: A practical quantum computer programming framework.* Dissertation for Colorado Technical University. (UMI#3391574)
- Cornell University Library articles on quantum physics, http://arxiv.org/archive/quant-ph
- http://en.wikipedia.org/wiki/Quantum_mechanics
- http://en.wikipedia.org/wiki/Quantum_computer
- http://www.dwavesys.com/en/dw_homepage.html
- http://www.networkworld.com/news/2011/092611-quantum-computing-250825.html?source=NWWNLE_nlt_daily_am_2011-09-26
- http://www.networkworld.com/community/blog/ibm-scientists-discuss-quantum-computing-breakthrough?source=NWWNLE_nlt_daily_am_2012-02-28

Thanks to grad students

- Matt Purkeypile
- Daniel Hars

Contact Info

- Bruce.Harmon@du.edu
- 303-871-6949