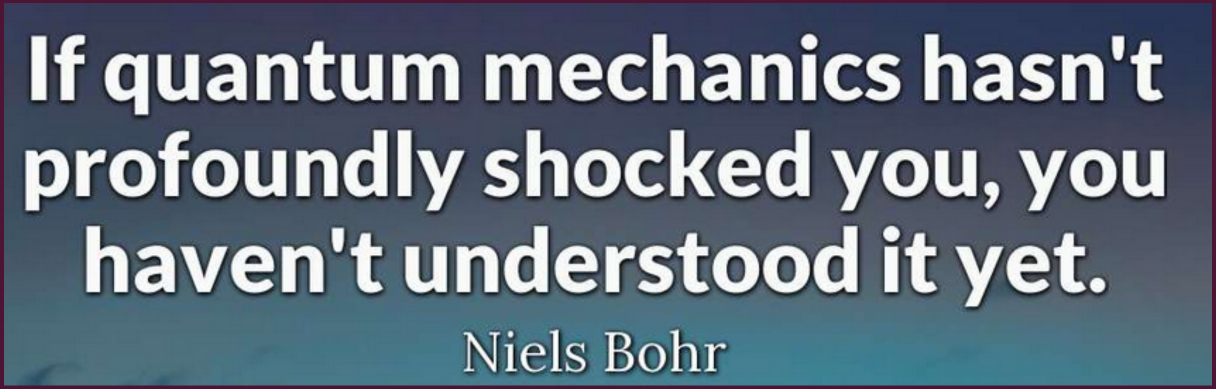
Quantum Computing and the Impact on CyberSecurity

THE CURRENT STATE

WITH DR. CHUCK EASTTOM

CHUCK@CHUCKEASTTOM.COM



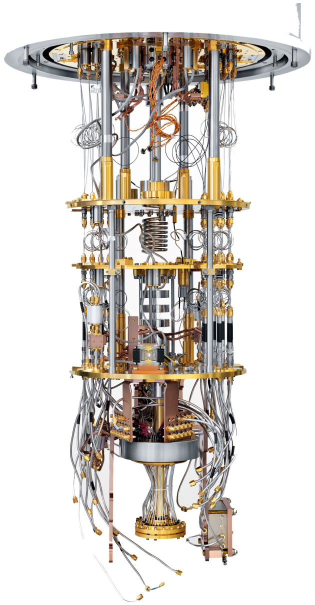
If quantum mechanics hasn't profoundly shocked you, you haven't understood it yet.

Niels Bohr

INTRODUCTION

What is a quantum computer?

A quantum computer is a machine that performs calculations based on the laws of quantum mechanics, which is the behavior of particles at the sub-atomic level.



THIS TALAK

- Defining quantum computing
- Exploring the impact
- Discussing current developments

WILL WE GET THERE

The March 2019 issue of IEEE Spectrum has an article by Mikhail Dyakonov. Dr. Dyakonov is a professor of physics at Laboratoire Charles Coulomb (L2C), Université Montpellier - CNRS in France.

IEEE SPECTRUM
FOR THE TECHNOLOGY INSIDER | 03.19
QUANTUM COMPUTING IS A MIRAGE
A PRACTICAL MACHINE MIGHT NEVER BE POSSIBLE P. 24
THE INTERNET OF COWS
HOW LoRa WIRELESS TECH MAKES IoT EASY P. 07
CHINA'S BID FOR GRID SUPREMACY
UPPING THE ANTE TO 1 MEGAVOLT P. 36
HERE'S HACKING'S STATE OF THE ART
BRANCH-PREDICTOR ATTACKS ARE ON THE RISE P. 42
EXCLUSIVE
SPECIAL DELIVERY
NIMBLE MACHINES WITH DYNAMIC LEGS WILL GO WHERE NO ROBOTS HAVE GONE BEFORE P. 30
IEEE

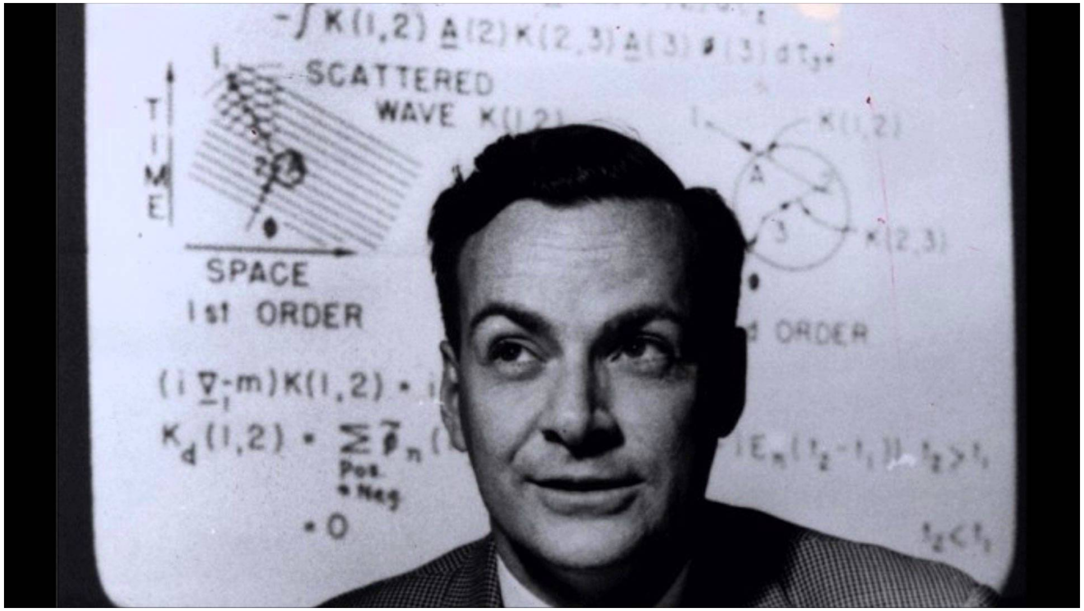
OVERVIEW

Most experts believe quantum computing will be a practical reality within the near future. When it does, all current, classical, asymmetric cryptography algorithms will be obsolete. This includes all the current algorithms used in e-commerce, online banking, and secure network communications. Therefore new cryptographic solutions must be found.

IBM CEO is opining that we are only 5 years from practical quantum computer.

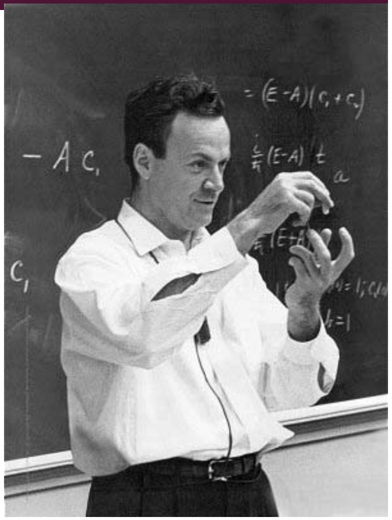
BACKGROUND

In 1982 Richard Feynman conceived of a “quantum mechanical computer"



INTRODUCTION

- "I think I can safely say that nobody understands quantum mechanics" - Feynman
- 1982 - Feynman proposed the idea of creating machines based on the laws of quantum mechanics instead of the laws of classical physics.
- 1985 - David Deutsch developed the quantum turing machine, showing that quantum circuits are universal.



- 1994 - Peter Shor came up with a quantum algorithm to factor very large numbers in polynomial time.
- 1997 - Lov Grover develops a quantum search algorithm with O(√N) complexity

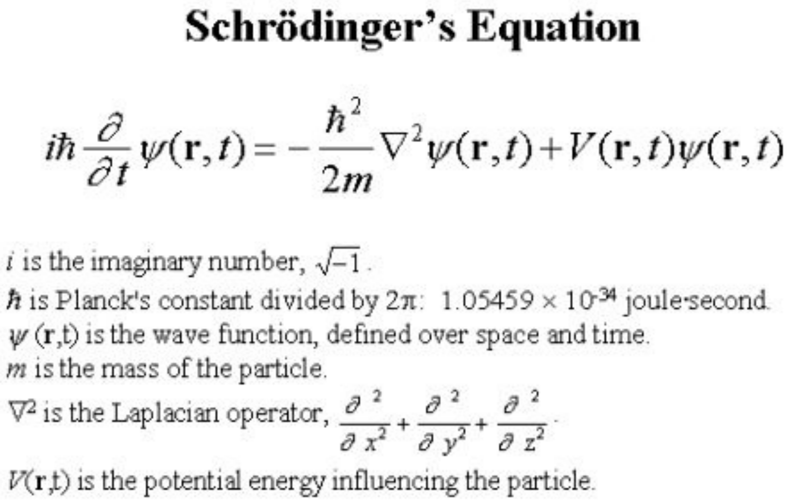
BACKGROUND

Peter Shor developed Shor's algorithm. On a quantum computer it can factor an integer N in polynomial time (actual time is log N). This is substantially faster than the most efficient known classical factoring algorithm (the general number field sieve) which works in sub-exponential time.

Peter Shor was awarded the Gödel Prize of the ACM and a MacArthur Foundation Fellowship in 1999

BACKGROUND

Quantum physics is largely probabilistic.

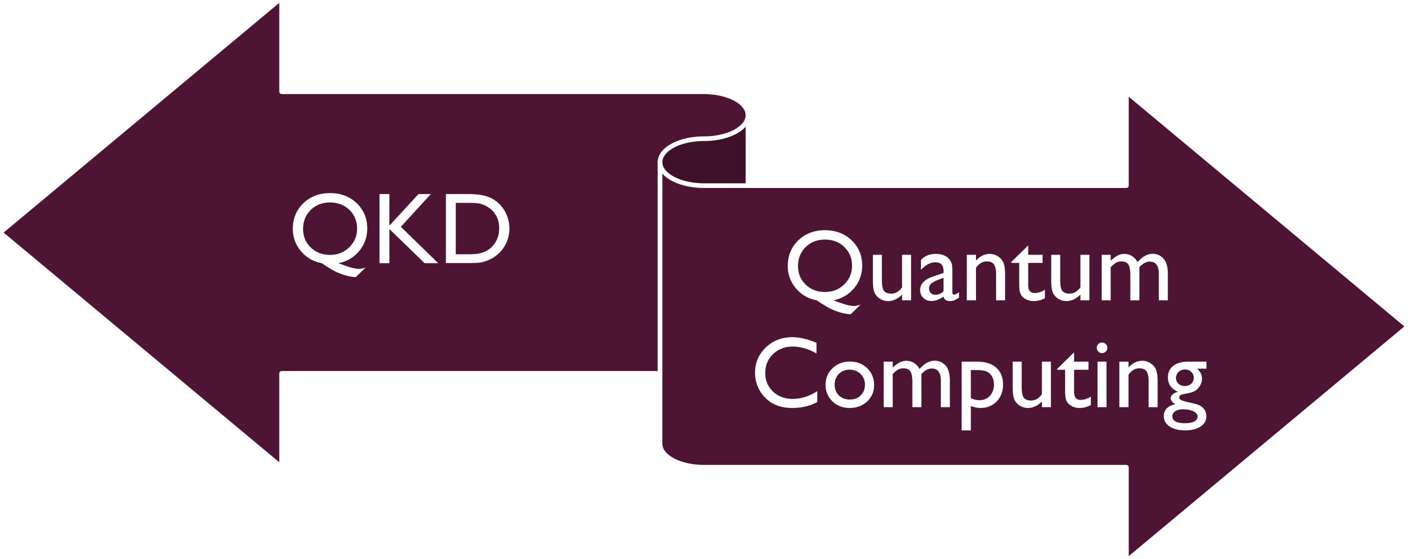


Schrödinger's Equation

$$i\hbar\frac{\partial}{\partial t}\psi(\mathbf{r},t)=-\frac{\hbar^2}{2m}\nabla^2\psi(\mathbf{r},t)+V(\mathbf{r},t)\psi(\mathbf{r},t)$$

i is the imaginary number, $\sqrt{-1}$.
$\hbar$ is Planck's constant divided by 2π: 1.05459×10^{-34} joule·second.
ψ ($\mathbf{r}$,t) is the wave function, defined over space and time.
m is the mass of the particle.
∇^2 is the Laplacian operator, $\frac{\partial^2}{\partial x^2}+\frac{\partial^2}{\partial y^2}+\frac{\partial^2}{\partial z^2}$.
V($\mathbf{r}$,t) is the potential energy influencing the particle.

TWO BRANCHES

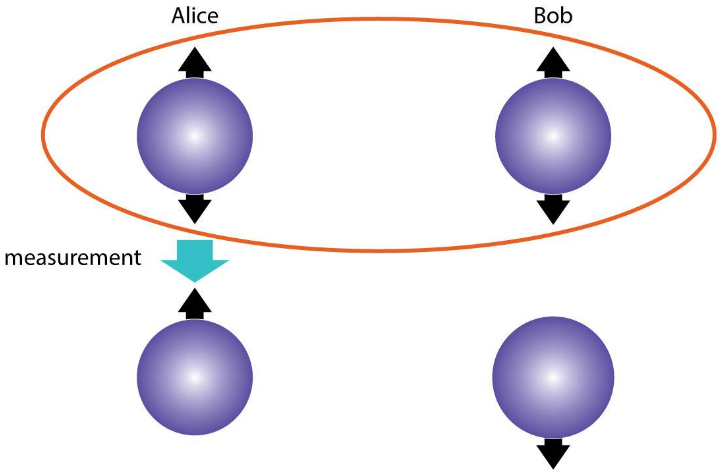


QKD

Quantum Computing

QUANTUM KEY DISTRIBUTION (QKD)

- Quantum entanglement
- BB84 protocol: Charles H. Bennett and Gilles Brassard (1984) uses photon polarization states to transmit information.
- The Six-state protocol, often simply called SSP was published by Bechmann-Pasquinucc and Gisn in 2019 in a paper entitled "Incoherent and Coherent Eavesdropping in the 6-state protocol of Quantum Cryptography
- E91 protocol: Artur Ekert (1991) uses photons that are entangled.



QUANTUM KEY DISTRIBUTION (QKD)

- Four companies currently offering QKD products
  - ID Quantique (Geneva)
  - MagiQ Technologies, Inc. (New York)
  - QuintessenceLabs (Australia)
  - SeQureNet (Paris).

TIMELINE

- 1994 Peter Shor’s algoirthm
- In 1998 Los Alamos Laboratory and Massachusetts Institute of Technology propagated the first qubit through a solution of amino acids
- The first two qubit machine was built by the University of California at Berkeley in 1998
- First five-photon entanglement demonstrated by Jian-Wei Pan's group at the University of Science and Technology of China, the minimal number of qubits required for universal quantum error correction in 2004.
- The Institute of Quantum Optics and Quantum Information at the University of Innsbruck in Austria developed the first qubyte (8 qubits) system
- 2006 First 12 qubit quantum computer benchmarked by researchers at the Institute for Quantum Computing and the Perimeter Institute for Theoretical Physics in Waterloo, as well as MIT, Cambridge
- Yale University created the first quantum processor in 2009

TIMELINE

- 2009 NIST demonstrates multiple computing operations on qubits
- 2011 D-Wave claims to have developed quantum annealing and introduces their product called D-Wave One. The company claims this is the first commercially available quantum computer
- 2012 D-Wave claims a quantum computation using 84 qubits
- 2012 Decoherence suppressed for 2 seconds at room temperature by manipulating Carbon-13 atoms with lasers
- 2014 Scientists transfer data by quantum teleportation over a distance of 10 feet (3.048 meters) with zero percent error rate
- 2015 D-Wave Systems Inc. announced on 22 June that it had broken the 1000 qubit barrier
- 2017 IBM unveils 17-qubit quantum computer
- 2017 IBM reveals a working 50-qubit quantum computer that can maintain its quantum state for 90 microseconds
- 2018 Google announced the creation of a 72-qubit quantum chip called "Bristlecone“
- 2018 Intel confirms development of a 49-qubit superconducting test chip, called "Tangle Lake"

TIMELINE

- January 2019 IBM unveils its first commercial quantum computer, the IBM Q System One.
- October 2019 IBM reveals a 53 qubit computer.
- February 2020 Quantum engineers report that they have created artificial atoms in silicon quantum dots for quantum computing and that artificial atoms with a higher number of electrons can be more stable qubits.e
- March 2020 Researchers report that they have found a way to correct for signal loss in a quantum node.

BUT WHAT DO WE NEED

These are rather general estimates. There are a lot of variables that effect these numbers:

- 100 qubits for quantum chemistry simulations
- 1000 qubits for effective machine learning
- 4000 qubits to factor 2048-bit RSA

CURRENT EXCITING TRENDS

- IBM's Q Network https://www.research.ibm.com/ibm-q/network/
- D-Waves Leap https://cloud.dwavesys.com/leap/
- Microsoft's Q# programming language https://docs.microsoft.com/en-us/quantum/language/?view=qsharp-preview
- There are quantum computing simulators https://quantiki.org/wiki/list-qc-simulators
- http://www.quantumplayground.net/#/home
  https://www.tomshardware.com/news/ibm-58-qubit-quantum-computer,39419.html
- Standards in the works including
  - P7130 – IEEE Standard for Quantum Computing Definitions
  - NIST Post quantum computing standard https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals

CURRENT EXCITING TRENDS

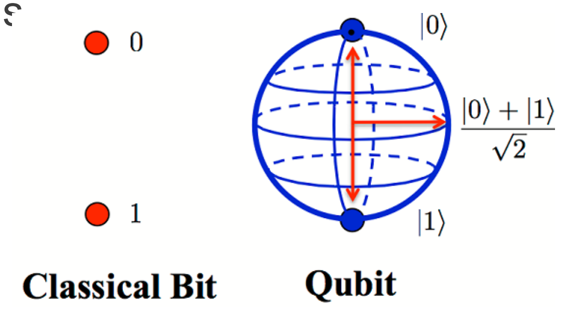
- IBM announced in 2019 their intent to commercialize quantum computing. They are working on a 58-qubit quantum computer. They are specifically considering it for AI applications.
- University of Chicago has a Quantum Exchange for Research

PROBLEMS FACING QUANTUM COMPUTING

The most prominent obstacle is controlling or removing quantum decoherence. This usually means isolating the system from its environment as interactions with the external world cause the system to decohere. However, internal factors in the quantum computer itself can cause decoherence.

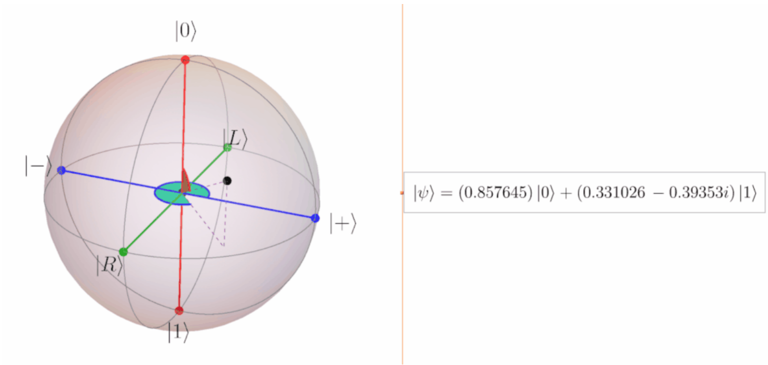
QUBITS AND QUANTUM GATES

A quantum circuit is essentially a sequence of quantum gates. It is reversible and is the analog of an n-bit register, called an n-qubit register.



A qubit is a two-state quantum-mechanical system. Spin or polarization work well. The qubit, unlike a bit, need not be in one state or the other, but is in a superposition of states.

The Bloch sphere representation of a qubit

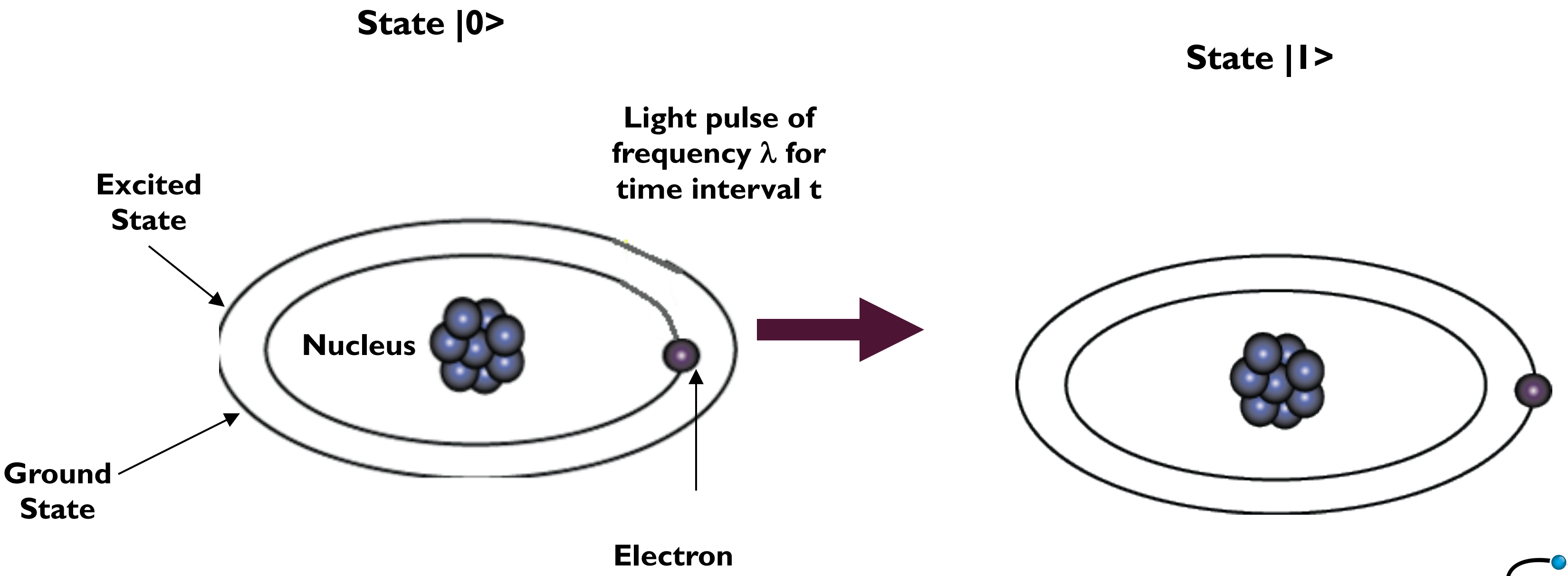


$|\psi\rangle = (0.857645)\,|0\rangle + (0.331026 - 0.39353i)\,|1\rangle$

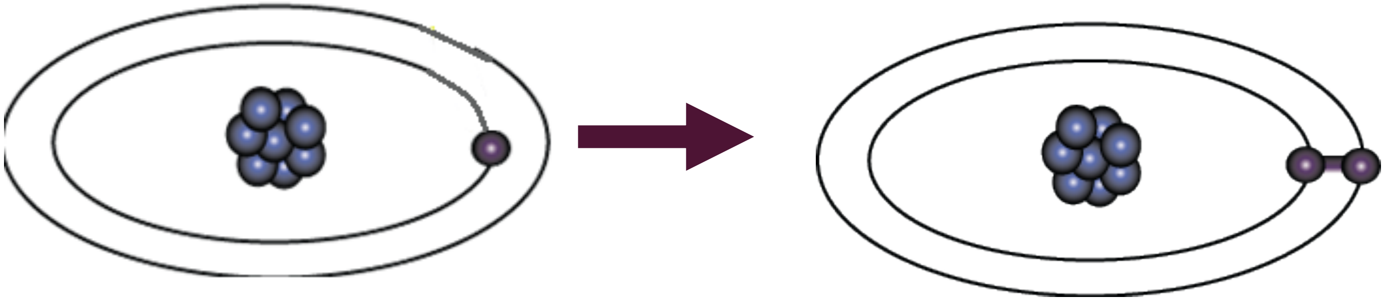
REPRESENTATION OF DATA - QUBITS

A bit of data is represented by a single atom that is in one of two states denoted by and . A single bit of this form is known as a ***qubit***

A physical implementation of a qubit could use the two energy levels of an atom. An excited state representing |1> and a ground state representing |0>.



REPRESENTATION OF DATA - SUPERPOSITION



Light pulse of frequency λ for time interval t/2

State |0>

State |0> + |1>

- Consider a 3-bit qubit register. An equally weighted superposition of all possible states would be denoted by:

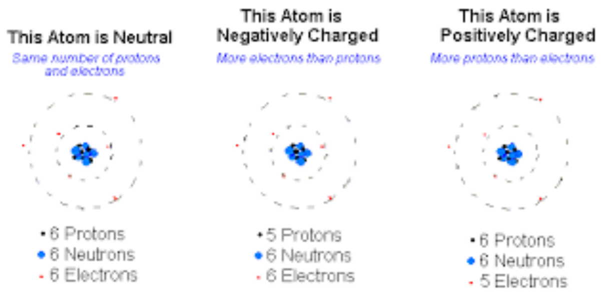
$$|\psi> = \frac{1}{\sqrt{8}}|000> + \frac{1}{\sqrt{8}}|001> + \ldots + \frac{1}{\sqrt{8}}|111>$$

HOW TO STORE THE QUBITS

IONS (used for quite some time)

A trapped ion quantum computer uses ions that are confined using electromagnetic fields. The Qubits are stored in stable states of each ion. Lasers are frequently used to manipulate the qubits.

The first implementation of a controlled-NOT quantum gate was proposed in 1995 by Ignacio Cirac and Peter Zoller and used the trapped ion system.


This Atom is Neutral
Same number of protons and electrons
• 6 Protons
• 6 Neutrons
• 6 Electrons
This Atom is Negatively Charged
More electrons than protons
• 5 Protons
• 6 Neutrons
• 6 Electrons
This Atom is Positively Charged
More protons than electrons
• 6 Protons
• 6 Neutrons
• 5 Electrons

HOW TO STORE THE QUBITS

Neutral Atoms (newer approach)

“Several research groups trap neutral atoms using either magnetic fields or light, but light traps have received the most attention for quantum computing. Atoms are polarizable, and the oscillating electric field of a light beam induces an oscillating electric dipole moment in the atom.”
-Weiss, D. S., & Saffman, M. (2017). Quantum computing with neutral atoms. *Physics Today*, *70*(7), 44.

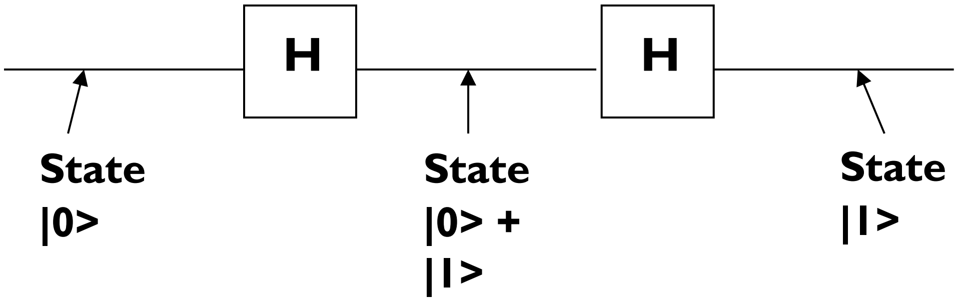
QUANTUM GATES

- Quantum Gates are similar to classical gates, but do not have a degenerate output. i.e. their original input state can be derived from their output state, uniquely. **They must be reversible.**

- This means that a deterministic computation can be performed on a quantum computer only if it is reversible. Luckily, it has been shown that any deterministic computation can be made reversible.(Charles Bennet, 1973)

QUANTUM GATES - HADAMARD

- Simplest gate involves one qubit and is called a ***Hadamard Gate (***also known as a square-root of NOT gate.) Used to put qubits into superposition.



State |0>

State |0> + |1>

State |1>

QUANTUM ANNEALING

Quantum annealing (QA). Quantum annealing is used mainly for problems where the search space is discrete (combinatorial optimization problems). Quantum annealing starts from a quantum-mechanical superposition of all possible states (candidate states) with equal weights. Then the system evolves with a time dependent equation (the Schrodinger equation).

Note: In metallurgy, annealing is a heat treatment that alters the microstructure of a material causing changes in properties such as strength and hardness. Commonly done by heating the material until it glows then letting it slowly cool to room temperature.

A LOT OF WORK DONE RECENTLY

- D-Wave systems produces quantum like computing systems that utilized quantum annealing
- In May of 2016 IBM made a quantum processor available to the general public via a cloud solution
- There are even programming languages developed for quantum computing

THINGS QUANTUM COMPUTERS DO WELL

- Solving integer factorization (Shor’s algorithm)
- Solving the Discrete Logarithm Problem
- Grover's algorithm searches a database using quadratically fewer queries to the database than that are required by classical algorithms.
- The Quantum algorithm for linear systems of equations or "HHL Algorithm", named after its discoverers Harrow, Hassidim, and Lloyd, is expected to provide speedup over classical counterparts

THE PROBLEM FOR CYBERSECURITY

The problem is that quantum computing will render most current asymmetric cryptography obsolete and there will be a need for cryptographic algorithms that are able to maintain security, even in light of quantum computing based attacks.

WHY

RSA – Factoring

DH – Discrete Logarithm

ECC - The discrete logarithm problem with respect to an elliptic curve.

Quantum computers can solve these problems in practical time.

NIST

Post quantum cryptography standards working group.

NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Full details can be found in the Post-Quantum Cryptography Standardization page.

The submission deadline of November 30, 2017 has passed. Please see the Round 1 Submissions for the listing of complete and proper submissions.

- In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of *post-quantum cryptography* (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.

- The question of when a large-scale quantum computer will be built is a complicated one. While in the past it was less clear that large quantum computers are a physical possibility, many scientists now believe it to be merely a significant engineering challenge. Some engineers even predict that within the next twenty or so years sufficiently large quantum computers will be built to break essentially all public key schemes currently in use. Historically, it has taken almost two decades to deploy our modern public key cryptography infrastructure. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing.

MAJOR APPROACHES

- Lattice based algorithms
- Multi-variate cryptography
- Supersingular elliptic curve isogeny cryptography
- Hashed based algorithms
- Code based algorithms

LATTICE BASED CRYPTOGRAPHY

Lattice based cryptography involves the construction of cryptographic primitives based on lattices. A lattice is represented by a standard matrix, familiar to anyone who has taken an introductory course in linear algebra. The vectors that constitute the lattice are known as the *basis vectors* for the lattice. A formal definition of a lattice is shown in the figure below.

$$\mathcal{L}\ (b1, ...,bn) = \left\{ \sum_{l=1}^{n} x_i b_i : x_i \in \mathbb{Z} \right\}$$

LATTICE BASED CRYPTOGRAPHY

Lattice based cryptography is simply cryptographic systems based on some problem in lattice based mathematics. One of the most commonly used problems for lattice based cryptography is the Shortest Vector Problem (SVP). Essentially this problem is that given a particular lattice, how do you find the shortest vector within the lattice? More specifically, the SVP problem involves finding the shortest non-zero vector in the vector space V, as measured by a *norm*, N. A *norm* is a function that assigns a strictly positive length or size to each vector in a vector space.

LEARNING WITH ERRORS (LWE) PROBLEM

This is a problem from the field of machine learning. It has been proven that this problem is as difficult to solve as several worst-case lattice problems. Put simply, this means that the LWE problem is very difficult to solve. The LWE problem has been expanded to use algebraic rings with Ring-LWE.

GGH ALGORITHM

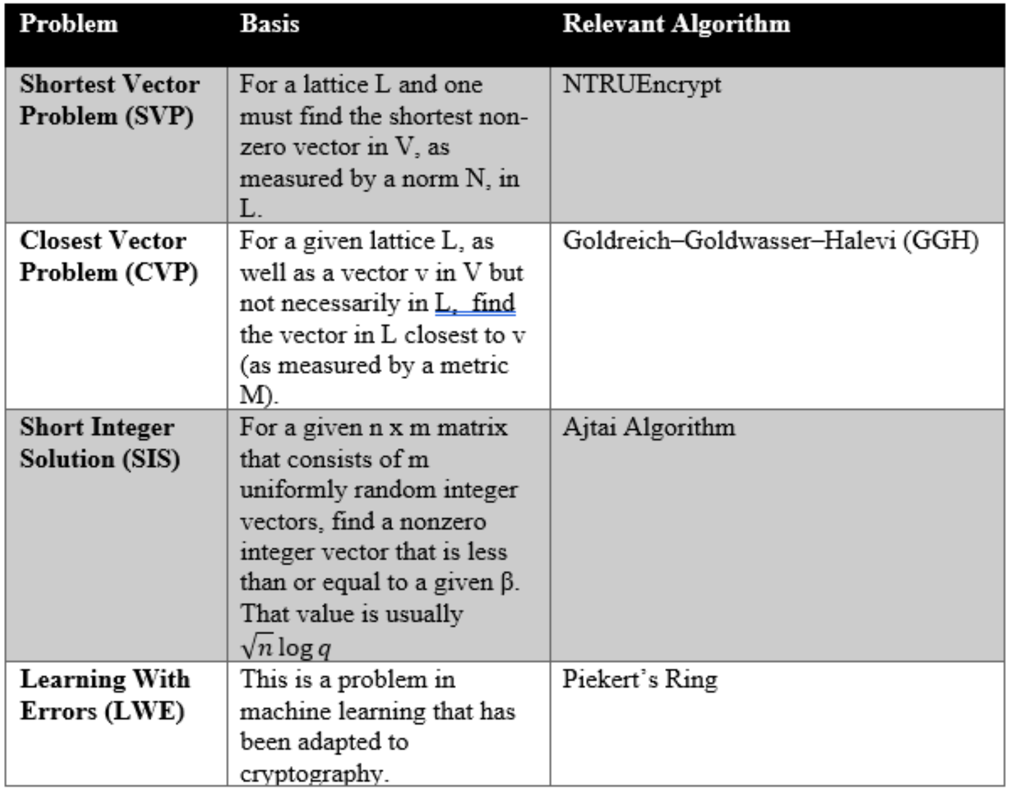
The GGH algorithm, named after its inventors Glodreich, Goldwasser, and Halevi (Peikert, 2016), is a lattice based crypto system. This algorithm was first published in 1997 and uses the closest vector problem (CVP). This problem is summarized as: given a vector space V, and a metric M for a lattice L and a vector v that is in the vector space V, but not necessarily in the lattice L, find the vector in the lattice L that is closest to the vector v.

$$v = \sum m_i b'_i$$

NTRU ALGORITHM

NTRU is another lattice based cryptosystem. It was invented by Hoffstien, Pipher and Sillverman. NTRU has been shown to be resistant to Shor's algorithm. Shor's algorithm is named after the inventor, Peter Shor, and it is a quantum algorithm for integer factorization. It is effective at factoring large numbers, thus breaking cryptography based on factorization problems. Another important fact about NTRU, is that even without concern about quantum computers, NTRU is more efficient than RSA. That makes it a viable option for classical computing.

OVERVIEW OF ALGORITHMS



Problem	Basis	Relevant Algorithm
Shortest Vector Problem (SVP)	For a lattice L and one must find the shortest non-zero vector in V, as measured by a norm N, in L.	NTRUEncrypt
Closest Vector Problem (CVP)	For a given lattice L, as well as a vector v in V but not necessarily in L, find the vector in L closest to v (as measured by a metric M).	Goldreich–Goldwasser–Halevi (GGH)
Short Integer Solution (SIS)	For a given n x m matrix that consists of m uniformly random integer vectors, find a nonzero integer vector that is less than or equal to a given β. That value is usually $\sqrt{n}\log q$	Ajtai Algorithm
Learning With Errors (LWE)	This is a problem in machine learning that has been adapted to cryptography.	Piekert's Ring

OVERVIEW OF CURRENT CRYPTANALYSIS

GGH has solid mathematics but has been the target of multiple, successful cryptanalytical attacks. The math is sound, but variations should be explored.

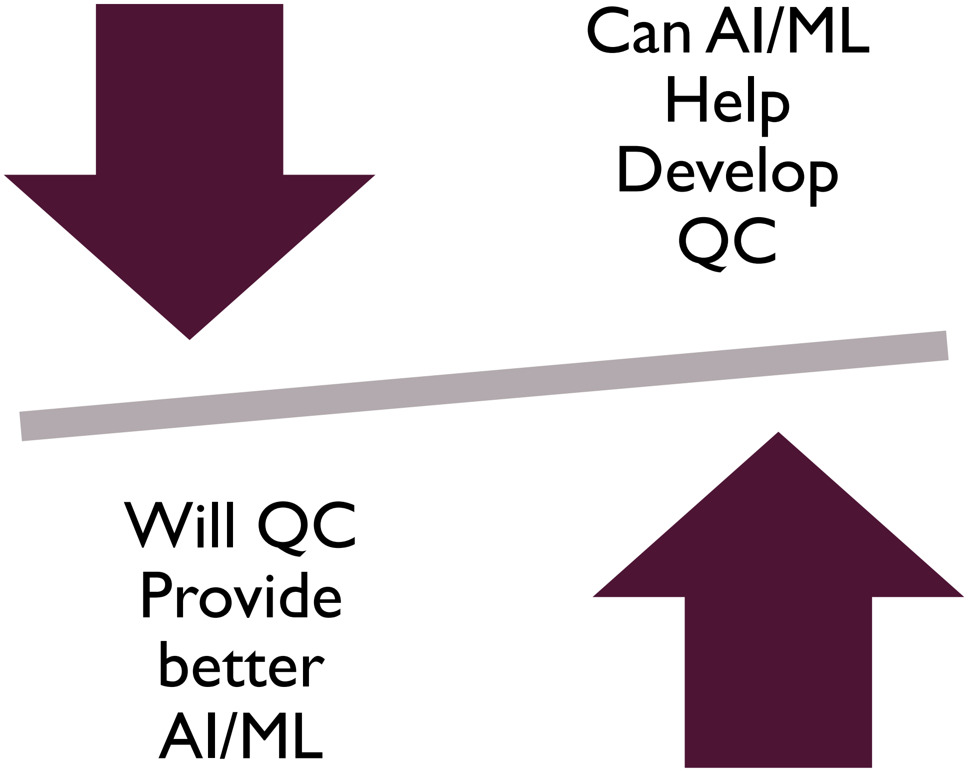
NTRUEncrypt appears to be robust as far as current cryptanalytical studies can determine.

LWE key exchange protocols have been found to be susceptible to several attacks. Further research is needed.

QUANTUM COMPUTING AND AI

What about quantum computing and machine learning/AI?

THERE ARE TWO PRIMARY ISSUES



Can AI/ML Help Develop QC

Will QC Provide better AI/ML

MACHINE LEARNING BASED ON GROVERS ALGORITHM

- Grover's algorithm is a quantum algorithm that finds with high probability the unique input to a black box function that produces a particular output value, using just $O(\sqrt{N})$ is the size of the function's domain. It was devised by Lov Grover in 1996 There are approaches to ML to improve it with quantum information processing uses amplitude amplification method.

QUANTUM MACHINE LEARNING

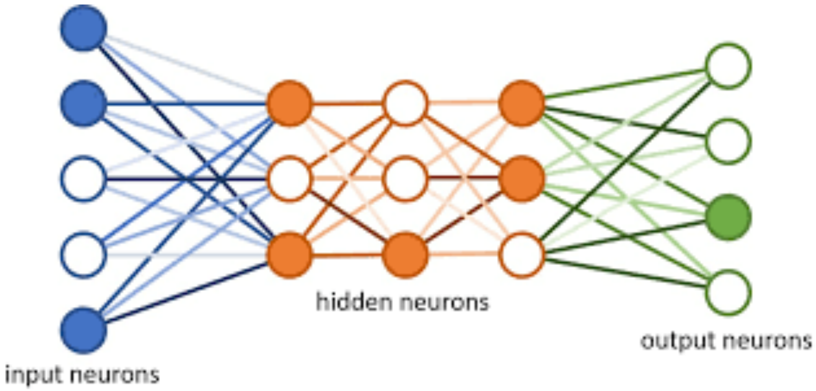
- Quantum-enhanced machine learning refers to quantum algorithms that solve tasks in machine learning
- The term "quantum machine learning" is often associated with classical machine learning methods applied to data generated from quantum experiments.
- This includes hybrid methods that involve both classical and quantum processing, where computationally difficult subroutines are outsourced to a quantum device.
- Quantum analogues of classical neural nets are often referred to as quantum neural networks.
- Hidden Quantum Markov Models (HQMMs) are a quantum-enhanced version of classical Hidden Markov Models (HMMs), which are typically used to model sequential data in various fields like robotics and natural language processing.

QUANTUM MACHINE LEARNING

- A number of quantum algorithms for machine learning are based on the idea of amplitude encoding, that is, to associate the amplitudes of a quantum state with the inputs and outputs of computations. Many quantum machine learning algorithms in this category are based on variations of the quantum algorithm for linear systems of equations.
- Another approach to improving classical machine learning with quantum information processing uses amplitude amplification methods based on Grover's search algorithm, which has been shown to solve unstructured search problems with a quadratic speedup compared to classical algorithms.

QUANTUM NEURAL NETWORKS

- Quantum Neural Networks are essentially ANN's based on quantum mechanics. There are primarily two major avenues of QNN research. One is the application of quantum information processing to improve neural network models. The to other approach involves looking for quantum effects in natural neural networks. The latter is most related to work by Roger Penrose.
- One common goal is a quantum equivalent for the perceptron unit. The perceptron is an algorithm for supervised learning of binary classifiers.



NOTEWORTHY PROJECTS IN QUANTUM-AI

- Google AI https://ai.google/research/teams/applied-science/quantum-ai/
- "Quantum Entanglement in Deep Learning Architectures," was published this in March 2019 in the journal Physical Review Letters.
- As early as 2018 scientists were reporting exciting results with Neural networks enabling learning of error correction strategies for computers based on quantum physics.
- Accenture, a global professional services company, has been granted a US patent for a "quantum computing machine learning module" that trains artificial intelligence (AI) to determine when and how computational tasks would be best handled by quantum computing versus classical computing methods, and route them to the appropriate option. US patent number 10,275,721 granted April 30, 2019

NOTEWORTHY PROJECTS IN QUANTUM-AI

“My colleagues and I instead hope to build the first dedicated neural network computer, using the latest ‘quantum’ technology rather than AI software,” wrote Michael Hartmann, a professor at Heriot-Watt University who’s leading the research, in a new essay for *The Conversation*. “By combining these two branches of computing, we hope to produce a breakthrough which leads to AI that operates at unprecedented speed, automatically making very complex decisions in a very short time.”

NOTEWORTHY PROJECTS IN QUANTUM-AI

- Speaking during a keynote at DesignCon 2019, Dr. Irfan Siddiqi, a professor of physics at the Quantum Nanoscience Laboratory and the Department of Physics at the University of California Berkeley, proposed artificial intelligence as a possible solution to the complexity of creating quantum computers.
- In September 2019 researchers at Harvard published work on a quantum circuit-based algorithm inspired by convolutional neural networks (CNNs). "The resultant quantum circuit involves only log(n) number of parameters to be optimized for n-qubit input data, which is double exponential improvement compared to a naive approach, in which exp(n) number of parameters are optimized,"

NOTEWORTHY PROJECTS IN QUANTUM-AI

- In October 2019 it was announced that the Wisconsin Quantum Institute Awarded Grant from the Department of Energy to Advance Quantum Computing Machine Learning.
- Schuld, M., & Killoran, N. (2019). Quantum machine learning in feature Hilbert spaces. *Physical review letters*, *122*(4), 040504. Their work is in reference to encoding inputs in a quantum state as a nonlinear feature map that maps data to quantum Hilbert space
- Cárdenas-López, F.A., Sanz, M., Retamal, J. C., & Solano, E. (2019). Enhanced Quantum Synchronization via Quantum Machine Learning. Advanced Quantum Technologies, 1800076. Uses machine learning to improve quantum synchronization.
- O'Driscoll, L., Nichols, R., & Knott, P.A. (2019). A hybrid machine learning algorithm for designing quantum experiments. *Quantum Machine Intelligence*, *1*(1-2), 5-15. Their work is on using machine learning to improve the design of quantum expiriments

CONCLUSIONS

Questions??

RESOURCES - SIMULATORS

- http://www.quantumplayground.net/#/home
- https://algassert.com/quirk
- https://www.ibm.com/quantum-computing/technology/simulator/

RESOURCES – QUANTUM COMPUTERS

- D-Wave https://www.dwavesys.com/take-leap
- IBM https://www.ibm.com/quantum-computing/

REFERENCES

- Albash, T., Rønnow, T. F., Troyer, M., & Lidar, D. A. (2015). Reexamining classical and quantum models for the D-Wave One processor. The European Physical Journal Special Topics, 224(1), 111-129.
- Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188-194.
- Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... & Smith-Tone, D. (2016). Report on post-quantum cryptography. US Department of Commerce, National Institute of Standards and Technology.
- Chi, D. P., Choi, J. W., San Kim, J., & Kim, T. (2015). Lattice based cryptography for beginners. IACR Cryptology ePrint Archive, 2015, 938
- Fano, G., Blinder, S. (2017). Twenty-First century quantum mechanics: Hilbert space to quantum computers: Mathematical methods and conceptual foundations. New York City, New York: Springer.
- Imre, S., & Balazs, F. (2013). Quantum computing and communications: An engineering approach. Hoboken, New Jersey: John Wiley & Sons.
- Kumar, R., Maurya, S. G., Chugh, R., & Manoj, P. V. (2014). Current refuge trends using classical and quantum cryptography. International Journal of Computer Science and Information Technologies, 5(3), 2974-77.
- Mariano, A., Laarhoven, T., Correia, F., Rodrigues, M., & Falcão, G. (2017). A practical view of the state-of-the-art of lattice-based cryptanalysis. IEEE Access, 5, 24184-24202
- Monteiro, R. T. (2016). Post-quantum cryptography: lattice-based cryptography and analysis of NTRU public-key cryptosystem (Doctoral dissertation). University of Lisbon, Portugal.

REFERENCES

- Moret-Bonillo,V. (2017). Adventures in computer science: From classical bits to quantum bits. New York City, New York: Springer.
- Peikert, C. (2016). A decade of lattice cryptography. Foundations and Trends in Theoretical Computer Science, 10(4), 283-424.
- Raychev, N. (2015). Quantum computing models for algebraic applications. International Journal of Scientific & Engineering Research, 6(8), 1281-1289.
- Rieffel, E., Polak, W. (2011). Quantum computing: A Gentle introduction. Boston, Massachusetts: MIT Press.
- Shenoy-Hejamadi, A., Pathak, A., & Radhakrishna, S. (2017). Quantum cryptography: Key distribution and beyond. Quanta, 6(1), 1-47
- Stanescu, T. (2016). Introduction to quantum matter & quantum computation. Boca Raton, Florida: CRC Press.
- Trabesinger, A. (2017). Quantum computing: towards reality. Nature, 543(7646), S1-S1.
- Wang, D. S., Hill, C. D., & Hollenberg, L. C. (2017). Simulations of Shor's algorithm using matrix product states. Quantum Information Processing, 16(7), 176-183.
- Easttom, C. (2019). "An Analysis of Leading Lattice-Based Asymmetric Cryptographic Primitives". 2019 IEEE 9th Annual Computing and Communication Conference.