Table Of Contents

1.1 Introduction to Quantum Computing: A Brief History of Quantum Mechanics

- 1900 Max Planck – Black Body Radiation – energy is quantized
- 1905 Einstein – Photo Electric Effect
- 1913 Bohr Model of the Atom
- 1925 Heisenberg's Matrix Mechanics
- 1926 Schrodinger's Wave Equation
- 1927/1930 Solvay Conferences – Einstein vs Bohr
- 1935 Einstein, Podolsky, Rosen paper
- 1964 Bell's Inequality
- 1982 Aspect experiments confirms Bohr's Quantum Mechanics is true versus Hidden Variables

1.2 Introduction to Quantum Computing: A Brief History Of Quantum Computing

- 1981 Feynman – Universal quantum simulator
- 1985 Deutsch – Universal quantum computer
- 1992 Deutsch-Josza Algorithm
- 1993 Simon's algorithm
- 1994 Shor's Algorithm – Factoring and Discrete Log
- 1996 Grover's Algorithm – Quantum Search
- 1997 Brassard, Hoyer - Amplitude Amplification
- 2002 Childs et. al. - Quantum Random Walks
- 2009 Harrow, Hassidim, Lloyd - Linear Equation Solving
- 2010 Cornwell - Amplified Quantum Fourier Transform

1.3 Introduction to Quantum Computing: Qubits

- How is 0 or 1 represented ?
- Physically - electron spin, polarization of a photon
- Logically using Dirac notation
- **Qubits** 0 and 1 are unit length vectors, ket 0 and ket 1
- $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
- $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- In a 2 dimensional vector space - Hilbert space
- $|0\rangle$ and $|1\rangle$ are orthogonal

1.4 Introduction to Quantum Computing: Superpositions

- A **superposition** is a **state** where sub-states exist simultaneously together with corresponding amplitudes
- Example superposition state of |0> and |1>:
- $|\psi\rangle = \sqrt{1/2}\ |0\rangle + \sqrt{1/2}\ |1\rangle$
- $\sqrt{1/2}$ is the **amplitude** of $|0\rangle$ and also of $|1\rangle$
- Amplitudes can be complex numbers
- Sums of squares of the modulus of the amplitudes is always 1 (a probability distribution) $|\psi\rangle = \sqrt{1/n}\ |0\rangle + \sqrt{1/n}\ |1\rangle + \sqrt{1/n}\ |2\rangle + \sqrt{1/n}\ |3\rangle + ... \rangle + \sqrt{1/n}\ |n-1\rangle$

1.5 Introduction to Quantum Computing: Unitary Operators

- States evolve by the application of **Unitary Operators**
- Unitary Operators preserve the length of the vectors (All vectors are length 1)
- Operations are reversible unlike classical computing
- **Quantum speed up** is due to the unitary operator acting on each element of the superposition at the same time
- Example: The Hadamard Transform $H=1/\sqrt{2}\ \begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
- $H|0\rangle = 1/\sqrt{2}\ \begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = 1/\sqrt{2}\ (|0\rangle + |1\rangle)$
- $H|1\rangle = 1/\sqrt{2}\ \begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = 1/\sqrt{2}\ (|0\rangle - |1\rangle)$
- The trick is to produce interesting fast Unitary Operators that can solve problems.

1.6 Introduction to Quantum Computing: Measurement

- A **Measurement** of the final state is made to obtain a probabilistic answer. The state or Wave Function “collapses” down to an answer.
- Example: Consider the state
- $|\psi\rangle = \sqrt{3}/4\ |0\rangle + \sqrt{1}/4\ |1\rangle$
- 0 has probability 3/4, 1 has probability of ¼
- Make a measurement to obtain 0 as the most probable (3/4 vs 1/4) answer to the problem
- However we could have obtained 1 if we were unlucky
- When analyzing a quantum algorithm it is important to know the probability distribution of the final state

1.7 Introduction to Quantum Computing: Quantum Algorithms

- Example general quantum algorithm:
- Perform a classical algorithm as a prerequisite
- Initialize the state in a quantum register $|0>$
- Apply a series of unitary operators $U_k \ldots U_2 \; U_1 \; |0>$
- These unitary operators are implemented in quantum circuitry in a quantum computer
- Make a measurement of the final state (a superposition) to obtain an answer to a problem with some probability
- Perform a classical algorithm using this answer to obtain a final answer to the problem
- Example unitary operators
  - Quantum Fourier Transform
  - Grover's Quantum Search

1.8 Introduction to Quantum Computing
Other features

- No Cloning Theorem (1982): It is not possible to make a copy of an unknown quantum state
- Reversibility: Quantum computations can be reversed (unless a measurement has taken place)
- Entanglement: A quantum state cannot be factored into a product of states.
  $|\psi\rangle = \sqrt{1/2}\ |00\rangle - \sqrt{1/2}\ |11\rangle$ (A Bell state) e.g. is not (|0>+|1>)(|0>-|1>)
- Decoherence: A quantum system interacts with its environment losing information.
- Quantum Error Correction: Protects a quantum system from the effects of decoherence
  - Shor's 9 bit code, Steane's 7 bit code, Laflamme's 5 bit code, Gottesman's Stabilizer codes
- Teleportation: Quantum information can be transported from one location to another using classical communication and previously shared quantum entanglement at the sending and receiving location.

2.1 Physical Implementation of Quantum Computers Trapped-Ion Qubits

- **Single Qubit Gates**
  - Speed: 12 μs
  - Fidelity: 99.9999%
- **Number of Single Qubit Gates**
  - 2000
- **Two Qubit Gates**
  - Speed: 100 μs
  - Fidelity: 99.9%
- **Qubit Numbers**
  - Seven fully controlled
  - Singles and pairs common
- (Oxford, Innsbruck, NIST, UMD, Sandia, Duke,…) (Ref: Paul Lopata (LPS))

2.2 Physical Implementation of Quantum Computers Silicon Qubits

- **Single Qubit Gates**
  - Speed: 30 μs
  - Fidelity: 99.9%
- **Number of Single Qubit Gates**
  - 400
- **Two Qubit Gates**
  - Speed: 130ns
  - Fidelity: 99%
- **Qubit Numbers**
  - Two Max (October 5th 2015 – first two qubit silicon logic gate using electron spin)
  - Only a few labs have demonstrated silicon qubits
- (Univ. New South Wales) (Ref: Paul Lopata (LPS))

2.3 Physical Implementation of Quantum Computers Superconducting Qubits

- **Single Qubit Gates**
  - Speed: 20 ns
  - Fidelity: 99.9%
- **Number of Single Qubit Gates**
  - 350
- **Two Qubit Gates**
  - Speed: 40ns
  - Fidelity: 99.4%
- **Qubit Numbers**
  - Nine fully controlled
  - Singles and pairs common
- (UC Santa Barbara, IBM, Univ. Chicago) (Ref: Paul Lopata (LPS))

3.1 Problem solving using Quantum Computers

- Reference: NIST Quantum Zoo - http://math.nist.gov/quantum/zoo/ (Stephen Jordan)
- This website contains a list of references to 262+ papers for solving problems on a quantum computer. Some example problems are given in the following table:

Problem	Who / When	Quantum Speedup
Factoring (RSA)	Shor 1994	Superpolynomial
Discrete Log (DH, ECDH, DSA, ECDSA)	Shor 1994	Superpolynomial
Searching	Grover 1996	Polynomial
Collision Finding	Brassard, Hoyer, Tapp 1997	Polynomial
Linear Systems	Harrow, Hassidim, Lloyd 2009 Ambainis, 2010	Superpolynomial
Subset Sum	Bernstein, Jeffery, Lange, Meurer 2013	Polynomial
Pattern Matching	Ramesh, Vinay, 2003 Montanaro 2014	Superpolynomial

4.1 Quantum Cryptography: QKD Protocols

- Quantum Cryptography refers to Quantum Key Distribution Protocols and Quantum Random Number Generation. The following table shows the development of QKD protocols.

No	Year	Name of Protocol	Principles	Applications	Authors
1	1984	BB84	Heisenberg Uncertainty Principle	It uses four Photo Polarization states to transmit the information	Bennett and Brassard
2	1991	E91	Quantum Entanglement	It uses entangled pairs of photons	Ekert
3	1992	BB92	Heisenberg Uncertainty Principle	Similar to BB84 except uses two polarization states rather than four	Bennett
4	1999	SSP	Heisenberg Uncertainty Principle	It is a BB84 protocol using 6 states rather than four	Bechmann-Pasquinucci and Gisin
5	2003	DPS	Quantum Entanglement	Uses a simple configuration, efficient time domain and robustness against PNS attack	Inhoue, Waks, Yamanoto

4.2 Quantum Cryptography: QKD Protocols

- Quantum Key Distribution Protocols (contd)

No	Year	Name of Protocol	Principles	Applications	Authors
6	2004	SARG04	Heisenberg Uncertainty Principle	BB84 protocol. More robust when using lasers. QBER is worse. Provides more security against PNS attacks	Scarani, Acin, Ribordy, Gisin
7	2004	COW	Quantum Entanglement	Works with weak coherent pulses at high bit rates. Tolerant against PNS attacks	Gisin, Ribordy, Zbinden, Stucki, Brunner, Scarana
8	2009	KMB09	Heisenberg Uncertainty Principle	Two bases are used for encoding zero and one.	Khan, Murphy, Beige
9	2012	S09	Public Private Key Cryptography	Massive key distribution between n-1 comuters and one key distribution center	Esteban, Serna
10	2013	S13	Heisenberg Uncertainty Principle	Random seed, asymmetric cryptography. Zero information loss	Serna

4.3 Quantum Cryptography
Quantum Random Number Generators

- Quantum random number generation
  - QuintessenceLabs qStream QRNG (Measurements of light)
  - ID Quantique Quantis QRNG (Measurements of light)
- Classical Entropy Sources
  - NIST's Random Beacon (512 bits per minute)
  - Intel RDSEED entropy source instruction (thermal noise)
  - Intel's RDRAND is a CTR_DRBG instruction that meets NIST SP 800-90 requirements (max throughput of 100 M/sec RDRAND instructions for either 16, 32 or 64-bit returned values)
  - /dev/random
  - /dev/urandom
  - Various proprietary entropy sources

5.1 Post Quantum Cryptography

- Classical cryptographic algorithms are weakened by the existence of quantum computers
- Post Quantum Cryptography – development of algorithms and protocols that are immune to quantum computer attacks
- Also called Quantum Safe Cryptography (ETSI) , Quantum Resistant Cryptography (NSA IAD)
- In this part of the talk:
  - Which FIPS Approved algorithms are affected by the existence of quantum computers?
  - What research areas are being investigated for quantum safe cryptography?
  - We need to plan the transition of the security infrastructure to quantum safe cryptography
  - Which conferences and workshops are for Quantum Safe Cryptography?
- Reference: ETSI White Paper on Quantum Safe Cryptography
  - http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

5.2 Post Quantum Cryptography

- FIPS 140-2 Symmetric Key Algorithms

FIPS Approved Algorithm	Key Length	Effective Key Strength / Security Level	
		Classical Computing	Quantum Computing
AES-128	128	128	64
AES-256	256	256	128
Triple-DES 192	168	168	84

5.3 Post Quantum Cryptography

- FIPS 140-2 Digital Signature Algorithms
  - Note: Fewer qubits are needed to break Elliptic Curve Cryptography (ECC)

FIPS Approved Algorithm	Key Length	Effective Key Strength / Security Level	
		Classical Computing	Quantum Computing
RSA 1024	1024	80	0
RSA 2048	2048	112	0
RSA 3072	3072	128	0
DSA 1024	1024	80	0
DSA 2048	2048	112	0
DSA 3072	3072	128	0
ECDSA-256	256	128	0
ECDSA-384	384	192	0
ECDSA-521	521	260	0

5.4 Post Quantum Cryptography

- FIPS 140-2 Key Agreement Techniques
  - Note: Fewer qubits are needed to break ECC

FIPS Approved Algorithm	Key Length	Effective Key Strength / Security Level	
		Classical Computing	Quantum Computing
DH 2048	112	112	0
DH 3072	128	128	0
ECDH-256	256	128	0
ECDH-384	384	192	0
ECDH-521	521	260	0

5.5 Post Quantum Cryptography

- FIPS 140-2 Hash Functions

FIPS Approved Algorithm	Digest Length	Effective Key Strength / Security Level	
		Classical Computing	Quantum Computing
SHA-1	160	80	80
SHA-224	224	112	112
SHA-256	256	128	128
SHA-384	384	192	192
SHA-512	521	256	256
SHA-512/224	224	112	112
SHA-512/256	256	128	128

5.6 Post Quantum Cryptography

- Quantum Safe Cryptography – Areas of Research
  - Code based crypto systems
  - Lattice based crypto systems
  - Hash based crypto systems
  - Multivariate crypto systems

5.7 Post Quantum Cryptography

- Transition the infrastructure to quantum safe cryptography
  - First need to research and develop quantum safe cryptography in an open transparent way
  - Second need a plan to transition the infrastructure over to the new cryptography
  - New Algorithms
  - New Protocols
  - New Key Sizes
  - What is the impact on vendors?
  - What is the impact on standards?
  - What is the impact on labs?
- NOTE: NSA IAD is recommending vendors no longer transition to Suite B cryptography but wait for the transition to quantum safe cryptography (they call it quantum resistant cryptography).

6. Quantum Cryptography Conferences

- NIST held their first post quantum crypto workshop in 2015 (April 2015, NIST, Maryland, USA)
  - http://www.nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm
- ETSI/IQC Workshop on Quantum Safe Cryptography (October 2015, Korea)
  - http://www.etsi.org/news-events/events/949-etsi-iqc-3
- International Conference on Quantum Cryptography (September 2015, Tokyo, Japan)
  - http://2015.qcrypt.net/
- Seventh International Conference on Post-Quantum Cryptography (February 2016, Japan)
  - https://pqcrypto2016.jp/
- Workshop on the Frontiers of Quantum Information and Computing Science (September 2015, University of Maryland, USA)
  - http://frontiers2015.quics.umd.edu/

7. Quantum Computing – Investment and Research

- North America
  - Institute for Quantum Computing (IQC) at Univ. Waterloo, Canada
  - DWAVE company Canada (2015 received $29m CAD)
  - Google + NASA have bought a DWAVE quantum computer (quantum AI Lab)
  - Lockheed Martin has bought a DWAVE
  - Intel invested $50m in 10 year partnership with a Dutch University
  - Microsoft StationQ at UCSB
  - NIST + UMD (Joint Quantum Institute (JQI))
  - USA Army Research Lab - Quantum Networks
- Europe
  - UK Gov investing 270m pounds over 5 years, Oxford University + others (2013)
  - UK $50m private investment in Cambridge Quantum Computing LTD (CQCL)
  - Switzerland idQuantique company (QKD, QRNG)
- Australia
  - Quintessencelabs company (QKD, QRNG)

8. The Future

- When will the first GPQC arrive? Within 5 years
- How much will it cost? $10,000,000
- How will it be programmed and who will program it?
  - Quipper like programming language
  - Will programmers need to have a knowledge of quantum computing? Yes!
- What commercial problems can be solved using GPQCs? TBD.
- What happens to classical computers and laptops? Will they bite the dust? No. Only a subset of problems can be solved faster on a quantum computer. Still need classical computers for large set of problem solving / surfing the internet.
- Quantum Safe Cryptographic Algorithms?
  - Start preparing staff now for the future – it is coming sooner than you think.

9.1 References

- The author has freely used information from the following sources:
  - https://en.wikipedia.org/wiki/Main_Page
  - http://arxiv.org/archive/quant-ph (archive of most quantum physics papers)
  - http://math.nist.gov/quantum/zoo/ (Status of problems solvable by quantum computers)
- Conferences and Workshops papers and presentations:
  - http://www.nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm
  - http://www.etsi.org/news-events/events/949-etsi-iqc-3
  - http://2015.qcrypt.net/
  - https://pqcrypto2016.jp/
  - http://frontiers2015.quics.umd.edu/

9.2 References

- Books:
  - Quantum Computation and Quantum Information (Nielsen and Chuang, 2000)
  - Quantum Computation (Lomonaco, 2000)
  - Quantum Information Science and its Contribution to Mathematics (Lomonaco, 2010)
  - Mathematics of Quantum Computation and Quantum Technology (Kauffman, Lomonaco, 2007)
  - An Introduction to Quantum Computing (Kaye and Laflamme, 2007)
  - Quantum Mechanics: The Theoretical Minimum (Susskind and Friedman, 2015)
  - Computing: A Gentle Introduction (Rieffel and Polak, 2014)
  - Quantum Computing for Computer Scientists (Yanofsky and Mannucci, 2008) Quantum Computer Science: An Introduction (Mermin, 2007)
  - Quantum Computing: From Linear Algebra to Physical Realizations (Nakahara and Ohmi, 2008)
  - Quantum Computing (Hirvensalo, 2001)
  - Quantum Computing (Gruska, 2000)

9.3 References

- Company Websites:
  - http://www.dwavesys.com/
  - http://www.idquantique.com/
  - http://www.quintessencelabs.com/

9.4 References

- Specific Papers:
  - Quantum Key Distribution Protocols: A Review (Singh, Gupta, Singh) 2014
  - ETSI White Paper on Quantum Safe Cryptography Oct 2014:

  http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

- PhD Thesis and Publications
  - Amplified Quantum Transforms, Cornwell, 2014 http://arxiv.org/abs/1406.0190
  - The amplified quantum Fourier transform: solving the local period problem (Quantum Information Processing Journal (Springer), Cornwell, 2013, Vol 12, Issue 2, pp1225-1253)

10. Questions?

- Contact Information:

David Cornwell, PhD
Cornwell_david@bah.com

410 684 6579

Address:
Booz Allen Hamilton
NBP 304
Annapolis Junction
MD 20701