Quantum Computing and Cryptography

The Current state

With Chuck easttom

chuck@chuckeasttom.com

About the Speaker

- 26 books (Including 3 on forensics, 5 on computer security, 1 on cryptology, 1 on penetration testing)
- Dozens of research papers (white papers, peer reviewed research articles, etc.) Many on Cryptography
- Over 40 industry certifications including many security certifications
- 2 Masters degrees (M.Ed. and MBA in Applied Computer Science)
- D.Sc. In Cybersecurity (in progress) Dissertation topic: A comparative study of lattice based algorithms for post quantum cryptography
- MSSE (Master of Science in Systems Engineering (in progress) University of Texas at El Paso
- 13 Computer science related patents including 2 on steganography
- Over 25 years experience, over 15 years teaching/training
- Helped create CompTIA Security+, Linux+, Server+. Helped revise CEH v8. Created ECES and OSCFE
- Frequent writer for 2600, frequent speaker at hacking conferences including Defcon. Research into cyberwarfare and malware.
- Member of IEEE, ACM, and IACR. Distinguished Speaker of the ACM
- Presents workshops talks at security conferences all over the world including Defcon, Hakon India, Hakon Africa, ADFSL, ISC2 Security Congress, SecureWorld, etc.

www.chuckeasttom.com

chuck@chuckeasttom.com

Overview

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.

Background

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

Background

"Although any calculation that can be performed on a classical digital computer could also be performed on a quantum computer, doing so would be foolish for most problems. It is much harder to manipulate and measure qubits than it is bits. But hard computational problems exist for which no efficient classical algorithms are known."

Weiss, D. S., & Saffman, M. (2017). Quantum computing with neutral atoms. *Physics Today*, *70*(7), 44.

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

The Church-Turing principle - "There exists or can be built a universal computer that can be programmed to perform any computational task that can be performed by any physical object".

Timeline

- 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 2004By 2000 IBM developed a 5-qubit system
- 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

- 2011 14 qubit register
- 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"

Problems facing quantum computing

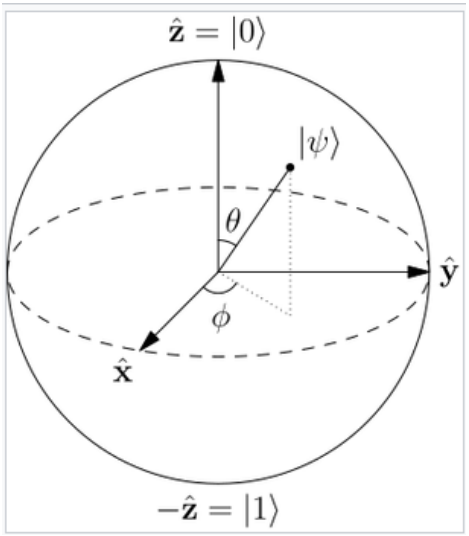
The most prominent obstacle is controlling or removing quantum decoherence. This usually means isolating the system from its environment as interactions with the external world cause the system to decohere. However, internal factors in the quantum computer itself can cause decoherence.

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

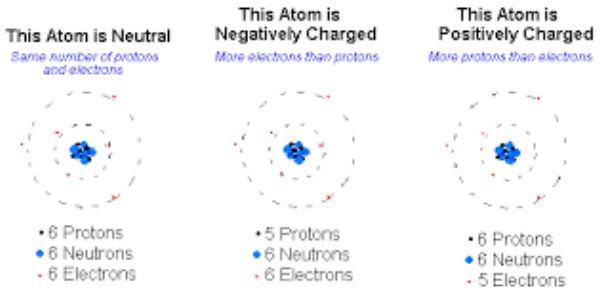


How to store the qubits

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.



How to store the qubits

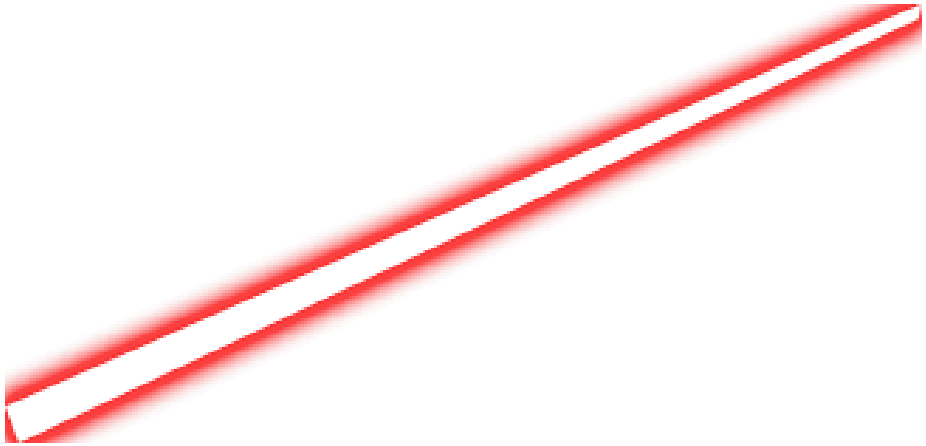
Neutral Atoms (newer approach)

"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.

Actual Techniques

Manipulating qbits with lasers
Manipulating qbits with microwave
Using both (Penn State)



Adiabatic quantum computation (AQC)

Adiabatic quantum computation (AQC) is a form of quantum computing which relies on the adiabatic theorem to do calculation.

First a Hamiltonian is found whose ground state describes the solution the problem of interest (i.e. what you are working on). Then a system with a simple Hamiltonian is initialized to ground state, and adiabatically evolved to the desired (and more complicated) Hamiltonian.

What is a Hamiltonian? You will see this a lot on quantum computing. It is an operator corresponding to the total energy of the system (at least in most cases). Often denoted by a H. Named after William Rowan Hamilton (1805 to 1865)

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.

Universal Quantum Gate

A universal gate quantum computing system relies on building reliable qubits where basic quantum circuit operations, similar to the classical operations that are common, can be put together to create any sequence, running increasingly complex algorithms.

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

The problem for crypto

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.

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 matrix is shown in the figure below.

$$A = \begin{bmatrix} 2 & 0 \\ -1 & 4 \end{bmatrix},$$

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.

GCH 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.

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.

Conclusions

- Quantum computing is coming, but nobody knows when.
- We need to have cryptographic solutions in place ready to implement.
- Even should quantum computing tarry…many of these algorithms may be more secure in classical computing.

Questions??

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.