Global Information Assurance Certification Paper

Quantum Computing and InfoSec

By Chris Weber
Tuesday, November 21, 2000

Introduction

Computers operating in the occult world of subatomic particles, performing calculations that embarrass our classical computers, may be the next step in the evolution of computer technology, and the start of a new wave of information security measures.

Forget everything you know about reality for a minute. Unless you are some sort of physicist, atom-smasher, or mathematics genius, **quantum theory** can seem like a bizarre blend of science fiction, mysticism, and magic. And minus a few sound and proven concepts, the theory is still unfolding.

Our present day lives are filled with computers of all shapes and sizes, different purposes, and an array of useful and not so useful features. The classical computer technology we use today is based on fundamental **bits**, which encode information as ones and zeros. Traveling across electronic circuits, bits are exchanged and manipulated typically in sequence, one by one.

Quantum computers will redefine what we know to be true. In their world, a quantum bit, or qubit, can be both a zero and a one simultaneously. Rather than a bit being represented by an electric pulse, or fibre optic photons, as we are used to, a qubit is represented by the spins of an atom. An "up" spin can represent a digital value of 1 while a "down" spin can represent a value of 0. But in the quantum world, the atom is capable of spinning in both directions **simultaneously**, thus allowing it to represent both 0 and 1 at the same time. If we can one day understand and make use of the quantum computer, we will move into a new era where entanglement, teleportation, and decoherence are readily understood.

The implications for computer security are amazing. On the one hand, quantum computers make it easy to crack codes that we currently depend on in our encryption methods and PGP keys. On the other hand, they present new opportunities for making secure data exchanges. With the field of quantum computing being so wide-open, the possibilities seem endless. There will most likely be new applications for quantum intrusion detection systems. A quantum firewall may not filter qubits, but rather allow access based on the laws of entanglement.

"Any sufficiently advanced technology is indistinguishable from magic."
- Arthur C. Clarke's Third Law

Classical versus quantum computing and information

Lets discuss how a classical computer differs from a quantum computer. Our

classical computers operate on technology that is over 160 years old. That's not bad, but there are doubts that Moore's law, which says that the number of transistors on a chip doubles every 18 months, will not last indefinitely. That is, as our computers get smaller and more powerful, we will have to enter the subatomic realm to make them work for us. "**Moore's Law** really runs out of steam, in the conventional sense, in 2012," Cherry Murray, director of Bell Labs Physical Research Labs says. "Once we start working with devices the size of atoms we get into the laws of quantum mechanics."[1] By 2012 we will already be working with transistors only three atoms thick.

In a classical computer, data is moved between processing elements, such as memory, hard disks, and peripherals, using metal wires. These metal wires are most often embedded into plastic boards or oxidized silicon wafers. All in all, these are the same wires that have been used for electric telegraphy since its invention by Sir William Fothergill Cooke, Sir Charles Wheatstone and Prof. Samuel F. B. Morse in 1837. [2] All three men submitted patents for the **electric telegraph** in that year.

The physical aspects of bits can vary depending on the medium. Across the metal wire bits are electrical pulses which represent an on or off state. Bits are either a one or a zero. Electric charge is either stored in a circuit or it isn't. A magnetic domain of the hard drive is either aligned with the direction of the head or it isn't. Things are cut and dry, and memory locations can be read without destroying the memory location.

The quantum computer does not follow these black and white rules. The world becomes blurred much as it does with fuzzy logic. The fundamental representation of data in a quantum computer is called a "qubit." The qubit is similar to the bit, but instead of being *either* a 1 or a 0, the qubit can be *both* a 1 and a 0 simultaneously. This phenomenon, known as "**superposition**," allows for a completely different approach to computing. With one qubit, you can manipulate two values at the same time. Add additional qubits and the power grows exponentially. With two qubits you can manipulate four values at the same time. If you could get up to 40 qubits, you can work with more than a trillion values simultaneously. In a classical computer, 40 bits gives you the same trillion plus values, but you can only work with them one by one.

Qubits are fragile for us to work with right now. Quantum information cannot even be read in its entirety, because the simple process of reading modifies the information. Quantum information can be *transferred* with perfect fidelity, but in the process the original information must be destroyed. Even more **drastic**, any measurement performed on a quantum system destroys most of the information in that system, and at least alters the state of the information. [3]

Logic is performed in any quantum computer when its qubit atoms affect the spin of neighboring qubit atoms. When structured properly, the quantum-computer atom can perform a number of mathematical operations in **parallel**.[4] With enough qubits, a very powerful computer can be constructed.

To reemphasize, the power of quantum computing comes from **quantum parallelism**. Classically, using parallel processors can decrease the time it takes to perform certain computations. To achieve an exponential decrease in computation time means an exponential increase in the number of processors and physical space. However, the amount of parallelism in a quantum system increases exponentially with the size of

the system. That is, an exponential increase in parallelism requires only a linear increase in the physical space needed.[5]

Quantum cryptography and code cracking

So what in the world could such fragile and infantile computers be used for? Even in their early years of invention, quantum computers are finding useful applications in the areas of computation and cryptography. A not so far off goal, and very important application, is to find the prime factors of very large numbers.

Prime factorization is not just a mathematical exercise. It is the foundation of cryptography and secure data exchange. It is fairly easy to multiply two prime numbers together – 5,456 and 8,976 for example. However, no one has found an easy way to do the calculation in reverse – finding a way to determine what two prime numbers can be multiplied together to equal 48,973,056. [6] This type of calculation takes a lot of time and a lot of power on our classical computers. But then came Peter W. Shor of AT&T Laboratories in Florham Park, NJ.

In 1994 **Peter W. Shor** came up with an awesome application for a nonexistent device. He created an algorithm that can find the prime factors of a large integer, a concept that goes straight to the heart of modern cryptography. For the first time, this algorithm has made factoring almost as efficient as multiplication. The trick is, that Shor's algorithm can only work by taking advantage of the unusual physics found only in a quantum computer, and the fast, parallel computations they make possible.

Around July of 2000, scientists at IBM Corporations Almaden Research Center in San Jose, led by quantum researcher **Isaac Chuang**, built a five-bit quantum computer and used it to perform calculations that take steps in Shor's direction.[7] Their five-bit quantum computer, squeezed onto a single molecule, is a big step forward. The five fluorine atoms in the molecule each represent a qubit, and make this computer the first ever capable of solving a problem related to code-cracking, the **order-finding problem**, in a single step. Every other computer in the world takes several steps to solve this problem. [8]

Now we see the power, uncertainty, and potential of quantum computing, so let's bring it a bit closer to home. We will look at one of our most common means of secure data exchanges – public-key cryptography.

Quantum public-key exchanges

Prime factorization is what makes public-key cryptography possible. People can send you secure messages that are encoded using the product of two prime numbers, but that message can **only be decoded** by someone who knows what those two prime factors are. Our computers automatically handle this coding and decoding. It is this method of security that occurs when we use PGP to encrypt our email messages, or when we perform secure online credit card purchases and financial exchanges.

Take our trustily secure **1024 bit** PGP keys for instance. With a classical computer today that performs millions of instructions per second (MIPS) during the

course of one year, a 1024 bit RSA key pair would take millions of years to crack! Now imagine a neural network of quantum computers, operating with thousands of qubits simultaneously and in parallel – the same 1024 bit key pair could be cracked in less than a year, maybe even months! (Note: a neural network in short is a system where processing elements can work in parallel)

So if some cracker is eavesdropping on your secure online transactions with their new Q1000 quantum computer, they could easily figure out the prime factors of incredibly large integers and crack the code.

"Thus, the development of quantum computers would require a complete change in the methods used to protect information transmitted over the **Internet** and other "secure" communications links."[9]

On the other hand, quantum computing presents cryptographers with new methods of guaranteeing secure data (within a negligibly small probability). As stated earlier, any measurement of quantum information inevitably disrupts the information itself(altering or destroying it). This seeming problem could be turned into an **opportunity** for computer security mechanisms, where any attempts made at eavesdropping on a message could set off alarms and stop the transmission.

Another opportunity for quantum cryptography, and an essential feature of quantum computing, is a strange property called **entanglement**. Einstein, Podolsky, and Rosen (EPR) first investigated entangled states in a famous paper called "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" This paper is noted by many as having launched Post-Modern Physics. Take two quantum objects (an electron or some other particle). These can be linked together so that by observing the state of one of the objects, you will know the state of the other object as well. This entanglement holds true over any distance, and according to EPR that can mean two particles on opposite sides of the planet, or even the universe.

So this brings up the phenomenon of "**action-at-a-distance**," often called quantum **teleportation**. The immediate thought is usually some "Star Trek" like teleportation system that transports objects from one place to another. But the reality of quantum teleportation is that we are teleporting information about the object, not the object itself.[10]

The possibilities for entanglement and cryptography are just being tapped. "Two people could encode information, trade it back and forth, and reconstruct the information using entangled quantum systems. Even if eavesdroppers intercept the coded information, they couldn't read the message because they wouldn't be part of the entangled system."[11]

Inside a quantum computer

One of the biggest questions still remains; can a useful quantum computer actually be built? Many innovative ideas of design have sprung up, but the most popular designs are based either on **ion traps** or on **nuclear magnetic resonance (NMR)**.

The ion trap quantum computer uses lasers to manipulate atoms and a chain of ions. Electric fields are used to confine a liner sequence of ions (qubits). Operations are

performed by using a laser on one qubit to create an impulse that ripples through a chain of ions to the second qubit. The ion trap approach is resource intensive, requiring an extreme vacuum and extremely low temperatures.[12]

The NMR quantum computer idea uses the spins of atoms. Using macroscopic amounts of matter, a quantum bit is represented by the average spin state of a large number of nuclei. The spin states are manipulated with magnetic fields and the average spin state can be measured with NMR techniques. The major problem is that this technique does not scale well. NMR computers have been successfully built with, just recently, 5 qubits. Many do not believe that they will scale well above 10 qubits. The major advantage of NMR is that it will work at room temperature.[13]

Decoherence is one of the biggest problems for building a quantum computer. This is the distortion of the quantum state caused by interaction with the environment. Basically, unless you could completely isolate the quantum computer from the environment, your system will be distorted by such factors as temperature, vibrations, electricity, etc. A popular method for dealing with this problem is by using error-correction techniques. In fact, quantum error-correction is an important field of study and provides one of the only methods that actually allow a quantum computer to be useful. Otherwise, the system will constantly produce unreliable information. With decoherence, the information contained in a quantum computer becomes altered or destroyed.

> "Building a real quantum computer is a viciously difficult task," says Isaac Chuang, . Everything depends on making sure the qubits retain their incredibly fragile quantum-mechanical mix of 1 and 0—what physicists refer to as staying "coherent." One bump from a stray air molecule, one twitch in the magnetic field, one ricochet of a random photon, and coherency vanishes. Let that happen in a quantum computer and your qubits will instantly collapse from *both-and* to *either-or*—meaning that you will suddenly find yourself looking at an ordinary computer full of ordinary 1s and 0s.[14]

The future

"Quantum computing today is at the point where classical computing was 70 years ago. We ponder on how to assemble very simple systems that can perform some very simple computations." [15] The systems being built today with five qubits are proving the concepts, but more powerful systems of thousands of qubits will be necessary to perform useful work. This type of quantum system may take form as a neural network of quantum computers operating in parallel, or a single quantum computer that can withstand all environmental interferences that make building a quantum computer so difficult today.

The realities are that this may very well be the next evolution in computing, making an extreme change from the singular computing technique we have all been using for the past 50 years – microchips based on the on-off dichotomy of binary logic. Systems are being built, and experts such as Shor believe that a 30 qubit system can be

made within the decade. There are many arguments that getting much beyond that will be technically impossible for years to come.

By that time, we will be facing new technologies that require methods of information security. But don't expect to trade in your PC for a quantum laptop in 2001, there is no telling when these systems would become portable and widespread, it could be more than 50 years.

When you ponder on the possibilities for information security, you realize there are no limits. We have seen the potential code-cracking and code-making abilities of the quantum computer. We will be forced to create new methods of symmetric-key and public-key cryptography systems. Secure Internet transactions may require quantum security measures that operate with the physical properties of qubits and subatomic particles, rather than a 1024 bit encryption key.

Intrusion detection systems may have to adapt to the quantum world in certain places. Instead of monitoring and filtering traffic, they may end up comparing the physical states of atoms and qubits to what is expected. A firewall system may go from a singular device to a neural network that allows access to quantum computers based on the laws of entanglement and teleportation. That is, two quantum firewalls on opposite sides of the globe may interact to allow qubits to pass based on the expected states of those qubits.

In reality, the widespread usage of quantum computers seems a long ways off (70 years or more), if it ever even becomes a reality. During that time, a quantum computer will only have real value in a few specific applications such as code cracking or database meta-searching. They will probably be expensive, and operated only by a few government agencies, and possibly large corporations. If there is to be any exchange of information between a quantum computer and a classical computer, devices will be needed to translate from qubits to bits as the data moves across the network.

The possibilities are endless, which is precisely why there is so much interest in quantum computing. Physicists and computer scientists are coming together to explore the new dimensions of possibilities. Everything mentioned in this paper could be completely turned upside down by the time a standard model of quantum computing is developed. But one thing is certain, this is the beginning of a new and radical change from the computers we know today, and the start of a quantum leap in computer technology as history will understand it. In the meantime, this is all (mostly) theoretical.

---

[1] Mckay, Niall. "The Next Tech Revolution." Infoworld Magazine. October 26, 1998. URL: http://www.britannica.com/bcom/magazine/article/0,5744,264142,00.html

[2] Buchanan, Robert Angus. The History of Technology. http://www.britannica.com/bcom/eb/article/9/0,5716,115399+20,00.html.

[3] Meglicki, Zdzislaw. "Introduction to Quantum Computing, B679." November 17, 2000. URL: http://ovpit.ucs.indiana.edu/gustav/B679/node9.html

[4] Johnson, R. Colin. "IBM quantum computer solves code cracking problem." October 22, 2000. URL: http://www.eetimes.com/story/OEG20000822S0007

[5] Riefell, Eleanor, and Polak, Wolfgang. An Introduction to Quantum Computing for Non-Physicists. (Xerox). August 14, 1998, p. 1.

[6] Boyle, Alan. "A Quantum Leap in Computing." MSNBC. May 18, 2000. URL: http://www.msnbc.com/news/269473.asp?cp1=1

[7] Moore, Samuel K. "Quantum Code Cracking Creeps Closer." IEEE Spectrum. October 2000. p. 18-19.

[8] Johnson, R. Colin. "IBM quantum computer solves code cracking problem." October 22, 2000. URL: http://www.eetimes.com/story/OEG20000822S0007

[9] Boyle, Alan. "A Quantum Leap in Computing." MSNBC. May 18, 2000. URL: http://www.msnbc.com/news/269473.asp?cp1=1

[10] Deutsch, David and Ekert, Artur. "Quantum Communication Moves Into the Unknown." Excerpt from Physics World. June 1993. URL: http://eve.physics.ox.ac.uk/qcweb/intro/comm.html

[11] Boyle, Alan. "A Quantum Leap in Computing." MSNBC. May 18, 2000. URL: http://www.msnbc.com/news/269473.asp?cp1=1

[12] Ibid

[13] Ibid. p. 4

[14] Waldrop, Dr. M. Mitchell. "Quantum Computing." MIT Technology Review Magazine. May/June 2000. URL: http://www.techreview.com/articles/may00/waldrop.htm

[15] Meglicki, Zdzislaw. "Introduction to Quantum Computing, B679." November 17, 2000. URL: http://ovpit.ucs.indiana.edu/gustav/B679/node7.html