Global Information Assurance Certification Paper

Quantum Encryption vs Quantum Computing: Will the Defense or Offense Dominate?
Bob Gourley
July 15, 2001

Quantum encryption will soon provide unbreakable ciphers. Quantum computers will soon allow the cracking of every cipher. Does something sound contradictory about those statements? The fact is we have a bit of a dichotomy here, and with teams on both sides of the argument fervently pushing their contradictory visions it can be hard for computer security professionals to separate the fact from the hype.

But that is what we are paid to do, and we have an obvious stake in how these technologies will change the future. This paper examines these topics by providing a snapshot of current research. We should start, however, with a short review of encryption today.

There are two basic types of encryption. Symmetric, or conventional encryption, and Asymmetric or public-key encryption. The vast majority of encryption today and almost all of the history of encryption has concerned symmetric encryption. It is called symmetric because both sides use the same key and the same algorithm to encrypt and decrypt messages. Since both sides know the key they can read the ciphertext created by the other side. Although even good symmetric encryption algorithms can be subject to brute force attacks (where every key is guessed), by making the key longer and longer this becomes harder for even super-computers to succeed at.

A problem with symmetric encryption has always been protection of the keys. If the key falls into the hands of someone else they can read the message or prepare their own messages with your cipher and spoof you. This has resulted in many very secure methods being created for key distribution and protection.

The other type of encryption-- Asymmetric or Public-Key-- is really new to the scene. This type of encryption was first made workable in 1978 by three researchers from MIT (Rivest, Shamir and Adlemen). Their method is now known as RSA encryption. Shortly after this another method was developed by Diffie and Hellman which is referred to as Diffie-Hellman key exchange. Although the actual algorithms and mathematical logic of these two methods differ, they both provide means where encryption can be established without both sides having access to the same key.

RSA provides a means where a user can post a public key for all to see while a private key is retained by the individual. Information encrypted with a users public key can only be read by use of the private key. Information encrypted with the private key can only be read by use of the public key. Diffie-Hellman uses other methods to enable two users to exchange a secret key in a secure way. With Diffie-Hellman, two users both post a public part of their key. Both users also have a private key. When user one wants to talk to user two securely, they need only perform functions on their public and private keys to derive a secure key that is unique to them and therefore unknown to others.

Diffie-Hellman is primarily used for key exchange. RSA, theoretically, can be used for encrypting any message, however, since its complex mathematical routines take a great deal of processing power, especially when used with large key lengths, it is primarily used for exchange of keys, after which a conventional encryption session is established. Although the mathematics associated with RSA are really beautiful to explore, that is not the primary focus of this paper. However, there is one aspect of the math involved in this type of system we must highlight-- RSA, like other public key systems, rely on mathematical functions that are believed to be have 'one way trap doors' in them. That is, it is the algorithm can be calculated one way, but it is computationally infeasible to reverse the calculation. For example, two very large prime numbers (for example, 100 digits long each) can be multiplied together to get an extraordinarily large number. But there are no known computationally feasible ways to factor that large number back into the two primes you started with. Another key must be used to assist in this. This is the 'trap

door' back to the ciphertext.

Quantum Cryptography and Quantum Computing can change all of the above. Here's a short introduction to these two terms before jumping into both in more detail.

Quantum Cryptography or Quantum Encryption is an emerging technology in which two parties may simultaneously generate shared, secret cryptographic keys using the transmission of quantum states of light. The security of these transmissions is based on the laws of quantum mechanics and theoretically secure pre and post transmission processing methods.

Quantum Computing describes research into new types of very powerful computers. Quantum computers will be able to perform functions on quantum particles which can represent both a zero and a one at the same time. As will be seen below, the potential calculating power of these computers is so significant it may well bring about yet another IT revolution.

QUANTUM ENCRYPTION

The goal of quantum encryption is to create encryption codes that are absolutely unbreakable and key distribution schemes that are un-interceptable. If this goal is met, the theorists say, quantum encryption systems will be virtually fail-safe against hackers since key distribution and key creation will be made far more safe.

The theory this technology is based on is extracted from the Heisenberg Principle, which asserts that at subatomic levels nothing can be measured without that measurement changing the thing being measured. Measuring that thing as it was without the act of measurement is not possible.

The first proposal for use of quantum encryption techniques to encode and decode information was made in the early 1980's by Gilles Brassard and Charles Bennett. They proposed a method that allowed a message to be sent using photons. Intercepting them and reading them would change them. This method involves special polarizing filters and previously agreed upon protocols, and the result is a successful key exchange that no intruder can exploit.

This type of quantum encryption technique has already been demonstrated. In fact, researchers at Los Alamos have shown that they can send secure messages through 48 kilometers of optical fibers and one mile of space.

Another key area of research is theories of "quantum entanglement." This refers to particles that even when far apart are linked together. Quantum mechanics holds that, until measured, a particle's properties can be in a combination of states, so a code derived from entangled photons could stay protected until "read" by both a sender and receiver.

Entangled quantum cryptography uses a specially prepared crystal to split a single photon into a pair of "entangled" photons. The polarization of each photon then becomes an undetermined state representing a mixture of both zeros and ones. Even when the entangled light particles are far apart, they influence one another's properties. Each photon could be detected either as a zero or a one, but once the polarization of one photon is detected, the second photon in the pair must assume a polarization that is identical to the first.

Recent advances in quantum entanglement were announced in April 2001 by three teams: a group from Los Alamos, a Swiss team and a joint German-Austrian team. The Swiss team used quantum entanglement to encrypt a message between two towns via fiber-optic lines. The German team encrypted and decrypted an image. The Los Alamos research team experimented with better ways to detect eavesdroppers who may threaten to alter the photon's properties in ways that can be detected via shifts in error rates.

This method of quantum entanglement may one day provide a way of instantaneous

communication that is un-interceptable, significantly changing the need for encryption.

QUANTUM COMPUTING

Quantum computers will be able to perform functions on quantum particles which can represent multiple states at the same time. Research teams consisting of computer scientists and particle physicists are designing systems that can calculate and test a virtual infinity of possibilities in parallel where modern computers would have to try each possibility serially-- one at a time.

The current concept behind quantum computing research involves the qubit or quantum bit. It is this qubit that can represent many different values simultaneously, allowing quantum computers to consider many variations. Qubits are coded by use of the spin of individual atoms.

A key concern of encryption experts is that a device like this will very likely allow computers to analyze and break public-key systems by trying all possible keys in parallel. Encryption algorithms such as RSA which rely on the difficulty of factoring large numbers into their primes will suddenly be obsolete, and everything ever encrypted by RSA will be at risk. If quantum computers become functional very little on the current day internet would be safe from cracking by the holder of this computer.

Do quantum computers really exist? They are already up and working-- but only in labs and only on a small scale. In March 2001 researchers at DoE labs reported they had demonstrated a seven-qubit quantum computer, which was a big experimental leap up from the previous benchmark of three-qubits. The first three-qubit demonstration was in 1998. This particular method uses nuclear magnetic resonance techniques and a drop of liquid.

Even with this latest advance, the world is still years away from a functional quantum computer. However, this recent development is a strong indication that quantum computing is quickly moving from the realm of science fiction into reality. When these computers become reality even the early versions will be incredibly powerful. A 30-qubit quantum computer would be roughly equivalent to a conventional computer running at 10 teraops, or trillions of operations per second. The fastest supercomputers in the world today have only achieved speeds of about two teraops.

The two technologies currently in use in laboratories to build experimental quantum computers are magnetic resonance and lasers. Experiments involving magnetic resonance manipulate particles in the atomic nuclei of molecules of a simple fluid (for example, trans-crotonic acid, which has six hydrogen and four carbon atoms). These particles behave like bar magnets spinning in a magnetic field that can be lined up by applying an electro-magnetic pulse from a nuclear magnetic resonance device. This lining up of spinning particles in positions either parallel or counter to the magnetic field allows the quantum computer to mimic the information encoding of bits in classic digital computers.

Quantum computer scientists believe they may someday be able to use nuclear magnetic resonance pulses of just the right frequency to manipulate or flip the quantum states of particles with sufficient reliability to create a functional quantum computer.

In other related research, in May of 2001, researchers at the University of Rochester demonstrated a way to effectively implement quantum computing techniques using laser technology. Like the nuclear magnetic resonance method described above, this technique is expected to be capable of conducting computations simultaneously. However, this system uses light instead of particles to drive the processing. It does so by imitating quantum interference, an important property that makes quantum computers exponentially faster at tasks. It does so by use of lasers. This design may prove to be as efficient as magnetic resonance quantum computers, but since it will be based entirely on light interference and light is easier to

manipulate, may be introduced far sooner than other quantum computing techniques.

For now, both of these technologies are in early stages, and they will certainly not become widespread for some time. But researchers continue to demonstrate that quantum computing is on the way.

A NET ASSESSMENT

The power of quantum computing will almost certainly lead to an ability to break modern day public key (asymmetric) encryption systems. It is just a matter of time. They will be broken by an ability to rapidly factor large numbers and more rapidly conduct brute force attacks. Conventional (symmetric) encryption systems that have any exploitable flaws will become child's play to break. Symmetric ciphers with small key lengths will also become breakable (the terms 'small' and 'large' have always been relative when it comes to encryption keys). However, quantum computing does not necessarily mean the end of encryption. As computers increase in speed, key lengths can increase dramatically. If we increase key lengths every time computing power increases, hackers, crackers, spies and thieves will stay behind the power curve. This means symmetric encryption is very likely here to stay.

A long-standing problem with symmetric encryption is key distribution. Public key encryption is our current solution to this age-old problem. But the technological advances of quantum computing now threaten that method. Quantum encryption, however, can allow for effective key distribution mechanisms. As quantum encryption technologies advance they will provide the ability to securely move encryption keys of any length, including keys as long as a one-time keypad. Even for quantum computers, a one-time keypad leads to an unbreakable cipher.

The research outlined above suggests that both quantum computing and quantum encryption are technologies that security professionals must begin to closely track. It also suggests that while quantum computing will very likely render most public-key encryption algorithms obsolete, it will only force us to use larger key lengths for traditional symmetric encryption techniques. The use of quantum encryption will provide secure paths for distribution of these larger keys, and, in some cases, will allow movement of messages in ways that cannot be intercepted, radically changing what needs to be encrypted.

Will quantum encryption provide unbreakable ciphers? Or will quantum computers allow the cracking of every cipher? There will likely never be a static, one time answer to those questions. All research to date indicates we should discount any claims that indicate an absolute answer. In fact, current research supports the conclusion that the constant struggle between the offense and the defense in the computer security business will always be with us.

REFERENCES

"The Future of Cryptography - Quantum Machines." [Online]. Available from http://www.cs.usask.ca/undergrads/dtr467/490/proj/future.shtml Accessed 11 Jul 01.

"You'd Have to Break the Laws of Physics to Break This Code" April 29, 2000 AIP [Online]. Available from http://www.aip.org/releases/2000/release03.html Accessed 10 Jul 01.

Diffie, W., and Hellman, M. "New Directions in Cryptography." IEEE Transactions on Information Theory, November 1976.

Harrison, Ann "Just Try To Crack This Code." June 19, 2000. IDG.net [Online]. Available from http://www.idg.net/go.cgi?id=276268 Accessed 10 Jul 01.

Hanson, Todd, "Lab scientists make seven bit quantum leap." Available from http://w10.lanl.gov:80/orgs/pa/News/032400.html. Accessed 9 July 01.

Rivest, R.; Shamir, A.; and Adleman, L. "A Method of Obtaining Digital Signatures andPublic Key Cryptosystems." Communications of the ACM, February 1978.

Stallings, W. Network Security Essentials: Applications and Standards. Prentice Hall. 2000. p.66-69.

Stenger, Richard, "Quantum-light processor may thrash supercomputers." May 17, 2001 [Online at CNN]. Available from http://www.cnn.com/2001/TECH/science/05/17/quantum.computer/index.html Accessed 13 Jul 01.