Johan Martinez
CIS 4930
4/23/05

INTRODUCTION

Intel co-founder Gordon Moore predicted in the sixties that transistor density on integrated circuits would double about every two years. This prediction has come to be known as Moore's Law, and forty years later, it has held true. However, if Moore's law is to hold true for the next forty years, computer chips must reach an atomic scale. Quantum Computing provides this atomic scale, thus it seems to be the next step for computers.

This next step may still lie decades away. However, scientists are already using Quantum Computing principles to strengthen a very specific area of cryptography. The technology that is being researched, and implemented is called Quantum Key Distribution, and it solves the cryptographic problem of providing a secure channel for the transmission of a private key.

Quantum Key Distribution (QKD) provides a secure channel for the transmission of a private key securely by encoding and transmitting the keys via photons. There are various protocols that have been devised for the distribution of keys with photons, two of which are BB84 and B92. These protocols rely on the fact that the act of observing or measuring a photon will change its orientation (polarization), thus the sender and receiver can be alerted of a possible eavesdropper. [2]

Quantum Key Distribution systems have already been successfully implemented both in the lab and at the marketplace. MagiQ Technologies and ID Quantique are the pioneers in the commercial field. They have both released products that make use of quantum technologies to implement key distribution. Successes in the lab include:

--The National Institute of Standards and Technology sent a quantum key over a 730-m free-space using infrared lasers, reflecting telescopes and 8-in.mirrors. [2]

--BBN Technologies boasts the world's first quantum network. It transmits quantum keys between BBN, Harvard University, and Boston University. [2]

The bulk of this paper will concentrate on QKD using photon polarizations and the BB84 protocol, which was devised by Bennett and Brassard in 1984. After the unveiling of QKD I will discuss the entanglement properties of photons and follow with a protocol published in a report sponsored by an agency of the United States. [8] To emphasize the practicality of these techniques, the last part of the paper will cite money invested into quantum technologies along with existing implementations of QKD and QKD products.

QKD: Physical System

QKD distributes encoded photons that represent a binary bit (0 or 1) through a fiber optic cable between a sender and a receiver, which I will refer to as Alice and Bob, respectively for the rest of this paper. In order to understand how a photon is encoded with a 0 or 1, you have to have a basic understanding of the wave properties of light.

Light is visible electromagnetic radiation. "In modern physics, light or electromagnetic radiation may be viewed in one of two complementary ways: as a wave in an abstract electromagnetic field, or as a stream of massless particles called photons."[4] The BB84 implementation of QKD actually uses single photons however, and one might be inclined to ask whether photons also possess wave-like properties. "Clearly, the polarization properties of light, which are more usually associated with its wave-like behaviour, also extend to its particle-like behaviour. In particular, a polarization can be ascribed to each individual photon in a beam of light."[5]

Among other properties such as electric and magnetic fields, electromagnetic waves possess a polarization. Paul A. Tipler describes polarization as follows in his Physics textbook: "We can visualize a polarization most easily by considering mechanical waves on a string. If one end of a string held horizontal is moved up and down, the resulting waves are polarized …. in the vertical direction." [6] The polarization of a wave can be vertical, horizontal, or can consist of a vertical component and a horizontal component. BB84 uses four polarizations to encode photons with either a 1 or a 0.

Polarization accounts for the encoding of a photon, but the laws of quantum physics enforce the security of the transmission a photon. A photon with a certain polarization can be detected by a filter that is setup to read photons with the given polarization. If the filter is not set up for this polarization however, not only might it not detect the right polarization of the photon, but it will also change its polarization in a random way [1]. This is vital for the security of QKD because it guarantees that if an eavesdropper Eve were to try to read the photons that Alice sent to Bob, Eve would have changed the polarizations of some photons. Through the BB84 protocol, Bob and Alice are able to tell if Eve was snooping on their transmission because of these changes in photon polarization.

QKD: BB84 Protocol

Suppose Alice wants to send a private session key to Bob in order to communicate securely via private-key cryptography over an insecure channel (the internet). In order to accomplish this, Alice and Bob must agree on the following:

A photon with a horizontal polarization represents a 0.
A photon with a 45 degree polarization represents a 0.
A photon with a vertical polarization represents a 1.
A photon with a 135 degree polarization represents a 1.

In addition, Alice must possess a photon transmitter that can transmit one photon at a time with one of the four polarizations discussed. Bob must possess two photon filters, or detectors, one of which is gauged to detect both horizontally and vertically polarized photons-represented by “+”-and the other of which is gauged to detect diagonally oriented photons in either diagonal polarization (45 degrees or 135 degrees)-represented by “x”.

Once the above is agreed on, Alice can begin transmitting the private key to Bob. Alice has to transmit photons to Bob in random polarizations, and record what polarizations she sent them in. On the other end, Bob has to use one of the two filters randomly on each of the photons Alice sends. Bob has to make sure to record the filters he used on each photon, and the polarizations he detected for each photon.

If the filter Bob uses is gauged for the correct polarization of a particular photon, then Bob detects the polarization of the photon accurately. If he uses the filter that is not gauged for the polarization of a particular photon, then Bob not only changes the polarization of that photon, but also detects a polarization that is not correct.

The rest of BB84 takes place over a conventional communication channel such as the internet. What happens next is Bob has to tell Alice the filter he used on each photon. Alice then has to reply to Bob telling him which photons were read correctly and should be kept. Both Alice and Bob then have to get rid of the photons which Bob read incorrectly. Once the incorrectly read photons are discarded, Bob and Alice should share an identical subset of photons, which when decoded into binary bits will give them a shared private key. Because Alice sends the photons in random polarizations, and Bob has a two filters, Bob has a 50% chance for each photon of reading it correctly, thus the shared private key will be consist of about half as many bits as the number of photons that were transmitted between Alice and Bob.

An eavesdropper cannot read all of the photons without changing them unless they know what polarizations Alice sent them in. Since Alice polarizes the photons in random fashion, the only alternative Eve had is to use one of the two filters randomly, and resend the photon to Bob. Eve will then change the polarization of 50% of the photons sent to Bob. When Bob measures the 50% of the photons which were changed by Eve, he will have a 50% chance of finding the original polarization that Alice sent for each of photon of this subset. This means that about 25% of the bits of the private shared key between Alice and Bob will be different once the protocol is implemented if there is somebody reading the photons in between them.

Alice and Bob can find this difference by comparing a subset of their shared key over a classical communication channel. If the difference in bits in the subset is 25% or greater, the keys are discarded and the protocol is started anew.

If the difference is less than 25%, they can discard the subset that was sent over the classical channel and keep the smaller shared key acquired from the implementation of the protocol.

QKD: Error Reconciliation

Even if Eve is not snooping in on the photon transmission, the polarization of some photons may be changed by noise caused either by the transmission and reception equipment, or by the communication medium. If noise changes the polarization of a subset of photons, Alice's and Bob's keys will not be matching bit strings as they should be. Two types of error reconciliation can be implemented in order to make the keys match. One is classical error reconciliation, which employs redundancy to eliminate errors. The other type is called Quantum Error Correction, which is radically different from the classical method. [9]

Entanglement: Weird Physics

Entanglement, a weird property of quantum mechanics which Einstein described as "spooky action at a distance" allows for another method of Quantum Key Distribution in which "the key comes into existence simultaneously at both sender and receiver nodes, eliminating the possibility of interception".[2] This type of QKD scheme is actually an improvement from BB84, because in addition to eliminating the possibility of interception, the scheme is also more practical, for current single-photon transmission equipment often transmits two photons(with the same polarization), which would make BB84 prone to attacks by Eve. The need for two photons in the entangled photons scheme allows for the photon equipment to operate more accurately.

Entanglement: Protocol for QKD

In order to implement the protocol, the following must be done prior to key distribution. Bob and Alice must agree on the bit representations of the four different polarizations, and on the two filters, just as they did with BB84. A photon source, other than Alice, must be established. This photon source will distribute entangled photon pairs, one photon to Alice and one photon to Bob. Alice and Bob must set their photon detectors to randomly select their filter for each photon.

To distribute the key, the source sends unpolarized entangled photons to Alice and Bob. An unpolarized photon is a photon whose polarization changes randomly as it propagates through space. Alice and Bob then both use their respective filters to measure the polarization of the photon. They document the value of the photon, the base used, and the time at which the measurement was made. Alice and Bob can then communicate over a classic channel to find out the instances in which their detection times coincided and they used the same base. "Due to entanglement, when measurement bases coincide, the bits are near 100% correlated and can be used to form a secret key" [8]

It is very important to realize that the sequence of bits that are read by both Alice's and Bob's photon detectors is a completely random sequence that is dictated by the fact that all of the photons are unpolarized. It is also important to note, that measuring a photon with the wrong filter of the two will give the photon one of the two polarizations on the filter in a random fashion, and that is the polarization the filter will detect. In other words, if the wrong filter is used on a photon, the filter cannot detect the polarization before it changes it.

If Alice and Bob both measure a distinct photon from the entangled pair with the same filter, their measurement will change their polarization to one of the two polarizations that the filter measures for, and if the photons are entangled, then there is a near 100% probability that both Bob and Alice will force the photon into the same polarization state. This will give them a shared bit that both Bob and Alice received simultaneously and whose value was completely random.

Implementations of QKD

QKD techniques are being used in labs around the world to distribute keys for use with private key encryption. "Last April(2004), a team from the University of Vienna, Austria's ARC Siebersdorf Research, and Ludwig Maximilians University performed the first quantum-secured transfer of money using entangled photons." [2] In addition to successful implementations sprouting up around the world, money is also sprouting to be used for QKD. "In April 2004, the European Union launched the SECOQC project, which involves 41 participants from 12 countries…..Participants have pledged 11.4 million euro ($14.8 million US) in funding over the next four years to create a secure quantum network globally." [2] The Department of Defense has also invested in the technology, "The DOD currently funds several quantum-cryptography projects as part of a $20.6 million initiative in quantum information." [2]

More importantly, QKD products are shrink-wrapped and on shelves, which is a sign of their practicality. On ID Quantique's website, you can find a press release dated April 25th, 2005 announcing the release of their new Vectis encryptor:

"*The Vectis link encryptor is a hardware Quantum Cryptography appliance for point-to-point wirespeed link encryption. It combines Quantum Key Distribution (QKD) and Advanced Encryption Standard (AES) encryption engines in a stand-alone unit. Key management, with key-refresh rates up to 100 times per second, and encryption are automated and their proper functioning is monitored by a surveillance unit*."[10]

Magiq's website boasts a press release dated March 28th, 2005, in which they announce the release of their QPN 7505 quantum encryption solution:

"The new platform incorporates several features to meet enterprise and government sensitive or classified requirements, including:

- *Multiple gigabit data plane for use in high speed networks*
- *Remote control for centralized network monitoring and management*
- *Multiplexing of data and quantum channel over a single fiber, reducing the operational cost of deployment"* [11]

Conclusion

Eve is in trouble. If Eve figures out a way to duplicate an RSA Diffie-Helman key exchange, and as a result is able to obtain the key, then Eve has probably figured out an efficient algorithm, or two perhaps, to solve two mathematical problems for which no efficient algorithms have been developed. This makes Eve's job pretty tough already. However, in order for Eve to obtain a key from a quantum key distribution system, Eve would either have to rewrite quantum mechanics, or create her own branch of physics.

Eavesdroppers may still have a chance though. Physics has contradicted itself in the past. Quantum mechanics, for example, contradicts the classical physics principle of locality. "Locality is the principle that an event which happens at one place can't instantaneously affect an event someplace else…..Aside from being intuitive, locality seems to be necessary for relativity theory, which predicts that no signal can propagate faster than the speed of light." [7] Einstein, Podolsky, and Rosen wrote a paper that showed the circumstances under which quantum mechanics violated the principle of locality. They didn't believe it could happen, and "viewed it as evidence that quantum mechanics was incomplete" [7]. Almost thirty years later, J.S. Bell proved with his theorem that if the circumstances which Einstein, Podolsky and Rosen wrote about were observed in an experiment and the results matched those of the predictions of quantum mechanics, then the principle of locality would not(exist) be a restriction in a quantum world. "Years later the experiments were done, and the predictions of quantum mechanics proved to be accurate." [7]

References:

[1] Guenther Cristopher. “The Relevance of Quantum Cryptography in Modern Cryptographic Systems”. GSEC Practical Requirements (v1.4b) Submitted: December 16, 2003

[2] Oullete, Jenifer. “Quantum Key Distribution”. The Industrial Physicist pg.22-25 December 2004/January 2005

[3] Goldwater, Sharon. “Quantum Cryptography and Privacy Amplification” http://www.ai.sri.com/~goldwate/quantum.html 12-10-96

[4] University of Tennessee. Department of Physics and Astronomy. http://csep10.phys.utk.edu/astr162/lect/light/waves.html

[5] Fitzpatrick, Richard. Fundamental Concepts of Quantum Mechanics.“The Polarization of Photons.” http://farside.ph.utexas.edu/teaching/qm/fundamental/node6.html 5-18-2002

[6] Tipler, Paul A. Physics for Scientists and Engineers. Fourth Edition Volume 2 Chapter 33 “Properties of Light”. W.H. Freeman and Company/Worth Publishers

[7] Felder, Gary. “Spooky Action at a Distance An Explanation of Bell’s Theorem. Copyright 1999. http://www.ncsu.edu/felder-public/kenny/papers/bell.html

[8] Kwuiat, Paul Rarity, John and Heinrichs Todd. Summary of Implementation Schemes for Quantum Key Distribution and Quantum Cryptography: A Quantum Information Science and Technology Roadmap. Part 2: “Quantum Cryptography”. Section 6.4: “Entangled Photons”. Produced for the Advanced Research and Develoment Activity (ARDA).

[9] “Quantum Error Correction”. www.wikipedia.com

[10] ID Quantique Press Rlease “Embargo: Monday April 25, 2005”. http://www.idquantique.com/news/files/release-vectis.pdf

[11] Magiq Technologies Press Release Magiq Technologies Announces New, Next Generation Quantum Cryptography Solution. http://www.magiqtech.com/press/MagiQ_7505.pdf