

Quantum Cryptography

Ryan Moore

MGT 6335

Manuel Mogollon

University of Dallas

Summer 2005

What is Quantum Cryptography?

- A method of securing communications using the properties of Quantum Physics
- QC relies on the Laws of Quantum Physics rather than complex mathematics to ensure confidentiality of information
- Utilizing features of Quantum Physics it is possible to design a communication system which is extremely secure
- QC is used as a key distribution method for traditional Symmetric Key cryptography
- Several QC commercial products have recently been developed and deployed

Development of Quantum Cryptography

- Quantum Cryptography was first proposed by Stephen Wiesner in his Paper “Conjugate Coding” published in SIGACT in 1983.
- Using Wiesner’s work, Bennett and Brassard created the first QC protocol, BB84, in 1984.
- The first experimental prototype based on their protocol was demonstrated in 1991.
- The major breakthrough realized by Bennett and Brassard was that photons could be used to transmit information but are not needed to store it.
- In 1990, Arthur Ekert, independently developed a different method of Quantum Cryptography based on Quantum Entanglement
- Only recently have technological advancements made it possible to produce a commercially viable QC product.

Quantum Theory

- Quantum Theory is counter-intuitive and often bizarre.
- A basic set of negative rules governs Quantum Physics.
 - It is not possible to measure the system without disrupting it.
 - It is not possible to simultaneously determine the position and momentum of a particle.
 - It is not possible to measure the polarization of a Photon in the Horizontal-Vertical basis and simultaneously in the Diagonal basis
 - It is impossible to draw a picture of an individual quantum process.
 - An unknown quantum state cannot be duplicated.
- Quantum Cryptography utilizes these principles in order to secure transmissions.

Quantum Cryptography Example

- Alice and Bob communicate over a Quantum System
- This can be accomplished by Alice encoding her information using Photons
- The Photons are then transmitted to Bob
- According to the first rule of Quantum Physics if the photons arrive undisturbed then no eavesdropping has occurred.
- Alice and Bob can verify this by exchanging a small random subset of the data over a public channel.
- This can only be determined after the fact so the most useful application of QC is for the exchange of keys for a traditional Cryptographic system.

Quantum Cryptography Methods

- Two methods have been developed for QC
- The first Method was proposed by Bennett, Brassard, and Wiesner and relies on The Heisenberg Uncertainty Principle.
 - Alice sends Bob Photons in one of 4 pre-agreed polarizations, 0, 45, 90, or 135 Degrees.
 - Because of the Laws of Quantum Physics Bob can either distinguish between the rectilinear polarizations (0, 90) or the diagonal polarizations (45, 135) but not both
 - Alice sends her photons with one of the 4 polarizations chosen at random
 - Bob chooses a random measurement for each photon but keeps his results secret
 - Bob then transmits to Alice, in the clear, what measurements, were used.
 - Alice transmits to Bob which measurements were correct.
 - Bob and Alice keep all cases in which the measurement was of the correct type
 - These cases are translated into bits (ones and zeroes), which then form the cryptographic key.
 - An eavesdropper (Eve) will always introduce errors into the system because of the laws of Quantum Physics
 - Alice and Bob can detect Eve by revealing a random subset of the key and checking the error rate
 - Eavesdropping cannot be prevented but it will always be detected.

Quantum Entanglement

- Arthur Ekert proposed a second method for QC using the properties of Quantum Entanglement
 - Quantum Entanglement states that two particles in a system will have observable and predictable correlations to each other even over a substantial difference.
- A sequence of paired photons with the same polarization are transmitted to Alice and Bob.
- Alice and Bob randomly vary the polarization they are detecting and record the results and times of detection.
- They inform each other of the times and the basis of each detection and keep the ones that match. This forms the key.
- An Eavesdropper would have to detect the photons, since the photons are “entangled” this would be easily detectable by Alice and Bob as the pair would have a different correlations when compared.

Privacy Amplification

- Errors and Background noise in a Quantum system will always be present.
- Because of the Uncertainty principle these errors may look like an Eavesdropper
- Privacy Amplification is employed to overcome this problem
- Privacy amplification is a method of creating secret shared information from a larger body of shared information that is only partially secret.
- Privacy Amplification functions with both the Brassard and Ekert Methods of QC
- Privacy Amplification can be done at the Quantum level with Ekert's method
- This is the method employed by QC commercial applications.

Commercial Products

- MagiQ
 - Quantum Key Distribution System
 - QC Encryption Appliances are placed at both ends of a fiber optic link.
 - Has a Range of 120km
 - Can be extended by daisy-chaining the appliances
 - Refreshes up to 100 Keys per second
 - Distributes keys for both 3DES and AES
 - <http://www.magiqtech.com/>
- IDQuantique
 - Vectis Link Encryptor
 - Encrypts standard Fiber Optic Links
 - Has a Range of 100 KM
 - Rotates through 100 keys per second
 - Distributes keys for 128,192, and 256 bit AES Encryption
 - <http://www.idquantique.com/>
- Both products use the BB84 QC algorithm

Quantum Cryptography in the Real World

- QC communication requires light to function therefore fiber optic links are necessary.
- This makes QC only viable over point to point links.
- Currently, qc is only used as a key distribution system.
- QC is only used for high-end, ultra-secure applications.
- Many Security Professionals do not see a need for QC.
 - Security is chain with many links
 - Cryptography is the strongest link in the security Chain.
 - Making cryptography stronger is not needed at this time.
- QC proponents respond by saying that as computing power increases QC will be needed as brute force attacks on Mathematical cryptography become more feasible.

References

- Bennett, "Quantum cryptography: Uncertainty in the service of privacy", Science, vol. 257, 7 August 1992, pp. 752 - 753.
- Bennett, Brassard, Bessette, Salvail, Smolin, "Experimental Quantum Cryptography", Journal of Cryptology, vol. 5, no. 1, 1992, pp. 3 – 28
- Ekert, Artur, "Introduction to Quantum Cryptography", <http://www.qubit.org/library/intros/crypt.html>, March, 1995
- "Quantum Cryptography", Wikipedia Article, http://en.wikipedia.org/wiki/Quantum_cryptography, June, 2005
- Schiener, Bruce, "Cryptogram", <http://www.schneier.com/crypto-gram-0312.html#6>, December 15th 2003.
- <http://www.magiqtech.com/>
- <http://www.idquantique.com/>