Global Information Assurance Certification Paper

Quantum Cryptography: A Primer
George H. Ackerman
Version 1.2e
September 5, 2001

"One cannot help feeling that cryptography at the beginning of the third millennium is still kept within a Black Chamber." F.L Bauer "Decrypted Secrets" Springer 1997

Introduction

Cryptography has been around since before the time of Caesar. Caesar, in fact, used his own cipher to send impolite jokes about people he knew to his friends. Cryptography has won wars by keeping battle plans secret and unreadable to the enemy.

Just when you thought the cryptography field was getting to the point where you actually understood the discipline, there is talk of a new player. This new participant that seems to be causing a stir is called Quantum Cryptography. While quantum cryptography is still several years away from mainstream use, there appears to be a growing interest in this attempt to connect the security of cryptography to the correctness of the Heisenberg Uncertainty Principal of quantum mechanics. Quantum cryptography depends more on physics as its cornerstone instead of traditional mathematics.

Quantum cryptography has its genesis with an idea formulated by Stephen Wiesner. In the 1960s Wiesner was a graduate student at Columbia University where he proposed the idea of quantum money. The beauty of quantum money is that it is impossible to counterfeit. Wiesner's concept suggested that paper currency have twenty "light traps" to capture and hold a photon. It was the initial manipulation and later verification of the photons and finally the comparison via a master list held by the bank that either accepted a bank note as authentic or rejected it as a counterfeit.

Classical Cryptography

To understand this cryptography of the future, it might be beneficial to review the concept of classical cryptography.

The reason we have cryptography is to prohibit an unauthorized person from intercepting and reading a message we have specifically sent to someone else. In the early days, this bit of magic was accomplished by keeping the entire encryption and decryption processes secret and shared only between the sender and the recipient. A good example would be the encryption process called the Block Cipher, also known as the Caesar Cipher or ROT Cipher. When a person knew that he would be receiving a message encoded using the ROT Cipher or for example ROT 13, the recipient of the message would know that each letter within the message had to be advanced by

thirteen letters in order to get to the text of the real message. Granted this might sound simple, but it was effective. Lets look at an example of ROT 13 using a well-known quotation:

"When cryptography is outlawed, bayl bhgynjf jvyy unir cevinpl." ("When cryptography is outlawed, only outlaws will have privacy") Anonymous

Today, instead of backing off a specific number of spaces as in the ROT Cipher scheme, we use something called a "key." A key contains the parameters of the encoding/decoding function. A key can be either public or private. The public key is used to encode plaintext, while the private key is used to decode the previously encoded plaintext or cryptogram. Lets look at this key concept in terms of a corner mailbox. Anyone can put a letter into the mailbox (public key holders), but only one person; the mailman (private key holder) can remove mail from the mailbox.

Now that we have our keys established, we can transmit our encoded message to the recipient via a medium. Its important to remember any standard key distribution can be passively surveyed without the knowledge of the intended users.

Quantum Cryptography: A Brief Introduction

The standard cryptography of today depends on sophisticated algorithms to keep prying eyes from intercepting and reading our messages. Even with the use of these algorithms, the total security of our messages can never absolutely be guaranteed. In quantum cryptography, we use the laws of physics for the exchange of keys to protect the confidentiality of our messages over an insecure channel. This ensures the security of our communication due to the fundamental quantum characteristics of light. To better understand how all of this works, we should start with an explanation of the concept of polarization.

Polarization

A photon can travel in any linear direction. While traveling along this linear direction, the photon will vibrate. This vibration can occur at any angle along its linear line of travel; however, the photon will always maintain the same angle of vibration. This vibration is known as the polarization of the photon.

At some point, it will become necessary for the receiver to begin the process of acceptance and rejection of the photons. Since photons vibrate in all directions, we will use a filter to accept the photons that maintain the same polarization. This filter is called a Polaroid.

With the use of several Polaroid filters, each requiring a different polarization, it now becomes possible to look for a pattern in a string of photons that someone has sent us. Once we have established our pattern, we can assign a predetermined "0" or "1" to any of our filtered photons and begin the process of encryption or decryption.

How Quantum Cryptography Works

Computer scientists and physicists Charles Bennett and Gilles Brassard considered the following explanation the “traditional” model they developed in 1984.

In their example of quantum cryptography, two people named Alice and Bob would like to establish a shared secret key they both can use to encrypt and decrypt a message being sent from Alice to Bob. This key would prevent a third person named Eve from intercepting and reading the message.

Alice has a polarizer that allows her to send out a stream of photons. These photons are assigned a value of “0” or “1” and are transmitted with a polarization filter in either a rectilinear or diagonal state.

At the other end of Alice’s transmission of photons, Bob must now measure each photon and determine which state Alice assigned to it as he receives each one. Now, here lies a problem. In order to determine the state of each photon as it is received, Bob has to decide to use either his rectilinear or diagonal polarizer filter. Since Bob doesn’t know in which state Alice sent the photons to him, he will obviously be wrong in some of his measurements.

Alice knows that Bob will make some incorrect measurements, so Alice contacts Bob via a telephone or another insecure medium. Alice informs Bob which Polaroid filter she used for the polarization of each photon during transmission; however, Alice does not divulge to Bob how each photon was polarized. For example, Alice will tell Bob that photon number 37 sent to him in the stream used a diagonal polarizer, but she will not tell him if the polarization was Upper left/Lower right or Upper right/Lower left. During this identification procedure, Bob will tell Alice if he used the correct polarizer for the reception of a particular photon. If Alice agrees that Bob used the correct polarizer for a specific photon, that photon is retained while incorrectly measured photons are rejected. At the end of this process, Alice and Bob have agreed on a secure one-time pad of 0s and 1s. As a result of eliminating the incorrect measurements, the new pad is considerably shorter than the original transmission Alice sent to Bob. They have not just created a relatively safe cipher; they have created a completely unbreakable cipher based on the laws of quantum physics. It should be noted that at this point Alice and Bob have created only the key and not the actual message. Now that the key is established we can finally begin the encryption of the message.

Now, lets say the third member of our example, Eve, wants to intercept and read the message. Eve will not be successful in her attempts, because the laws of quantum physics will prevent her from doing so. These laws, and more specifically, the added benefit of intrusion detection (accomplished by incorrectly measuring the photon and disrupting it), alerting Alice and Bob that someone has been eavesdropping on their transmission. Lets look at how this might be accomplished.

Eve will have to measure the photons the same way Bob made his measurements. While eavesdropping, Eve will have to decide weather to use either the rectilinear or diagonal detector. In making her choice, probability indicates she will be wrong 50% of the time in choosing the correct detector. Additionally, Bob has the advantage of comparing measurements with Alice and doesn't have to be concerned about any incorrect measurements. Remember. Alice either confirms or denies the results of Bob's measurement. Even if Eve "listens-in" to Alice and Bob's conversation regarding the correct measurements, this information will prove useless. It will prove useless for two basic reasons. Firstly, when Alice informs Bob of the correct measurements, she will select several random samples and not a complete reading of her transmission. Secondly, Eve will have used the wrong detector in some of her measurements making her interpretation of the transmission unreliable. Also, even if Eve was successful in reading the polarization of a photon, the act of looking at or inspecting the quantum information will disturb it and alert Alice and Bob of an interloper.

The basic steps of our process are as follows:

1. Alice transmits a series of polarized photons to Bob.
2. Bob attempts to measure the photons with his detector.
3. Via a random sampling, Alice tells Bob which of his measurements were correct.
4. Bob discards the incorrect measurements.
5. Alice and Bob have now created their key.
6. If Alice and Bob agree that their onetime pad is correct, they can start their encryption process. If they detect an interloper, they must start the process over again.

Practicalities

In 1988 Charles Bennett and John Smolin set out to prove that quantum cryptography was more then just a theory and was really workable. One night Bennett and Smolin assembled all of their equipment and cloistered themselves in a laboratory void of all light so that no wandering photon would interfere with their experiment. By early the next morning they were able to transmit photons across their laboratory in what was to be the first exchange of data using quantum cryptography. While the computers used for the experiment were only 30 centimeters apart, this was nonetheless an historic step for the future of cryptography and the quest for an unbreakable key.

It has been reported by SearchHP.com, a Hewlett-Packard related portal, that photons have been successfully transmitted over a distance of 60 kilometers. This was accomplished with the medium of very pure fiber optic cables. It appeared that after 60 kilometers, because of microscopic impurities and the Heisenberg Uncertainty Principal, further distances became unfeasible.

Can it be Cracked?

Before we address the question “can quantum cryptography be cracked?” It must first become an accepted technology. Until the quantum computer becomes a reality jeopardizing all modern ciphers, there really is no great need to make quantum cryptography a necessity. After all, The RSA cipher currently offers us unbreakable encryption.

What makes a quantum computer such a threat to today’s ciphers? Simply, due to its tremendous power, it has the ability to calculate and answer more than one question at a time. Let’s look at it this way. Today’s ordinary computer can answer only one question at a time. If you were to ask your computer two questions, you would have to enter each question individually. And individually is the same fashion in which your questions would be answered. In short, the computers of today operate by the laws of classical physics. In 1985, a British physicist named David Deutsch advanced his theory that computers should adhere to the fundamental laws of quantum physics. With the utilization of quantum physics, it would be possible to process two questions simultaneously rather than individually.

Apparently, the question we should be asking ourselves is “what will come first?” The quantum computer, which will have the power to break today’s ciphers or perhaps quantum cryptography, which will protect our ciphers from the quantum computer.

As mentioned earlier in this paper, quantum cryptography is a proven reality and is far more advanced then the quantum computer.

In Conclusion

In the near future, the eloquence and the absolute safety of quantum cryptography will allow it to become an accepted member of the Information Security family. It is at this stage that the art of cryptography will be at its zenith and the future of cryptanalysis will be in question.

Glossary

Caesar Cipher or ROT Cipher: The process of creating a code by advancing the letters of a message by a specific number of letters.
Cryptanalysis: The process of breaking codes and ciphers.
Cryptogram: Plaintext that has been encoded.
Cryptography: The process of creating codes and ciphers.
Diagonal: Upper left/Lower right or Upper right/Lower left
Key: Specific parameters used to encode and decode plaintext.
Plaintext: The text to be encrypted.
Heisenberg Uncertainty Principal: Formulated in 1927 by Werner Heisenberg. This is a succinct statement of the "uncertainty relation" between the position and the momentum (mass times velocity) of a subatomic particle, such as a photon. This relation has profound implications for such fundamental notions as causality and the

determination of the future behavior of an atomic particle.
Photon: A minute energy packet of electromagnetic radiation.
Polarization: Light waves travel in a linear direction and the vibrating electric vector associated with each wave is perpendicular to the direction of travel.
Polaroid Filter: A special filter used to measure polarized light.
Rectilinear: Up/Down or Left/Right
RSA Cipher: A widely used cipher developed by Rivest, Shamir, and Adleman. The RSA cipher, developed in 1977, is considered virtually unbreakable.
Quantum Computer: A computer based on quantum physics. It will have the capacity to calculate more the one problem at a time.

References

1. "Quantum Mechanics – The Uncertainty Relations." American Institute of Physics. URL: http://www.aip.org/history/heisenberg/p08.htm. Retrieved: (29 August 2001).
2. "Quantum Cryptography: Secure Communication over Insecure Channels." IBM at Almaden. URL: http://www.almaden.ibm.com/st/projects/quantum/crypto. Retrieved: (23 August 2001).
3. Bauer F.L. (Springer, 1997). "Quotes by Leading Cryptographers." D&G Sciences. URL: http://www.dgsciences.com/fwcc/quotes.htm. Retrieved: (2 September 2001).
4. Larchuk, Tod. (22 September 1994) "About Quantum Mechanics." California State University, Chico – College of Engineering, Computer Science & Technology. URL: http://www.ecst.csuchico.edu/~atman/Crypto/quantum/quantum-crypto-inf.html. Retrieved: (22 August 2001).
5. "Question 110. What is Quantum Cryptography?" IKS (Information Communication System) URL: http://www.iks-jena.de/mitarb/lutz/security/cryptfaq/q110.html. Retrieved: (23 August 2001).
6. "What is Quantum Cryptography?" Center for Quantum Computation. URL: http://www.qubit.org/intros/crypt.html. Retrieved: (22 August 2001).
7. Pawliw, Borys. (31 July 2001). "Quantum Cryptography." Search HP.com. URL: http://searchhp.techtarget.com/sDefinition/0,,sid6_gci284012,00.html. Retrieved: (22 August 2001).
8. "Cool Quotes Collection." Sleepwalker.net. URL: http://www.sleepwalker.net/quotes/index.php?p=quotes&cid=laughs, Retrieved: (2 September 2001).
9. Singh, Simon (1999). The Code Book. New York: Anchor Books.

Multiple-choice questions

Circle the letter that best answers the question.

1. Stephen Wiesner developed the theory of

    a. Quantum Physics.
    b. Quantum Cryptography.
    c. Quantum Money.
    d. Quantum Computers.

The correct answer is c. Quantum Money.

In the 1960s, while a student at Columbia University, Wiesner proposed the idea of quantum money.

2. A Polaroid is a type of

    a. Photon.
    b. Filter.
    c. Cipher.
    d. Transmission.

The correct answer is b. filter.

A Polaroid is a type of filter used to measure the polarization of a photon.

3. The polarization of a photon is determined by

    a. its speed of travel.
    b. its direction of travel.
    c. the angle of its vibration.
    d. the amount of heat it generates.

The correct answer is c. the angle of its vibration.

As a photon travels in a linear direction, the angle of vibration that it maintains is known as the polarization of the photon.

4. In their original 1988 experiment proving quantum cryptography, the computers used in the exercise were placed

    a. 1 kilometer apart.

b. 90 meters apart.
c. 400 centimeters apart.
d. 30 centimeters apart.

The correct answer is d. 30 centimeters apart.

In 1988 Charles Bennett and John Smolin set out to prove that quantum cryptography was more then just a theory and was really workable. While the computers used for the experiment were only 30 centimeters apart, this was nonetheless an historic step for the future of cryptography and the quest for an unbreakable key.

5. The computer we use today can work on

a. one problem at a time.
b. several problems at a time.
c. no more then three problems at a time.
d. several problems if they are coded correctly.

The correct answer is a. one problem at a time.

Today's computer can answer only one question at a time. It is the quantum computer and it's use of quantum physics that will allow a computer to work on more then one problem at a time.

True/False Questions

6. Cryptography has been around since the time of Caesar.

True False

The correct answer is True

Caesar would use his own code now known as the Caesar Cipher to encrypt/decrypt messages.

7. A key can be either public or private.

True False

The correct answer is True.

The public key is used to encode plaintext, while the private key is used to decode the previously encoded plaintext or cryptogram.

8. Quantum cryptography uses the laws of mathematics to protect messages.

True False

The correct answer is False.

In quantum cryptography, we use the laws of physics for the exchange of keys to protect the confidentiality of our messages over an insecure channel.

9. The quantum computer is much closer to mainstream use then quantum cryptography.

True False

The correct answer is False.

As mentioned early in the paper, quantum cryptography is a proven reality and is far more advanced then the quantum computer

10. The RSA cipher is an insecure method of encryption.

The correct answer is False.

A widely used cipher developed by Rivest, Shamir, and Adleman. The RSA cipher, developed in 1977, is considered virtually unbreakable.