Karen Hunter
SCI 510: Quantum
Todd Duncan
12/9/02

Quantum Cryptography

Spies, communication, and secret codes! Cryptography is the art of encoding and decoding messages and has existed as long as people have distrusted each other and sought forms of secure communication. The purpose of cryptography is to transmit information such that only the intended recipient receives it. Although the field of cryptography is ancient, it is not static. Cryptographic techniques have evolved over the centuries, with the code-makers working to stay ahead of the code-breakers. The next major step in this evolutionary process may be at hand. Today's most common encryption methods are threatened by the potential creation of the quantum computer. But already quantum cryptography has been developed which promises more secure communication than any existing technique and cannot be compromised by quantum computers.

Quantum cryptography takes advantage of the unique and unusual behavior of microscopic objects to enable users to securely develop secret keys as well as to detect eavesdropping. Although work on quantum cryptography was begun by Stephen J. Wiesner in the late 1960's, the first protocol for sending a private key using quantum techniques was not published until 1984 by Bennett and Brassard.

The development of quantum cryptography was motivated by the short-comings of classical cryptographic methods, which can be classified as either "public-key" or "secret-key" methods.

Public-key encryption is based on the idea of a safe with two keys: a public key to lock the safe and a private key to open it (Ford, 2002; Ekert, 1995). Using this method, anyone can send a message since the public key is used to encrypt messages, but only someone with the private key can decrypt the messages. Since the encrypting and decrypting keys are different, it is not necessary to securely distribute a key. The security of public-key encryption depends on

the assumed difficulty of certain mathematical operations, such as factoring extremely large prime numbers. (Ford, 2002).

There are two problems with basing security on the assumed difficulty of mathematical problems. The first problem is that the difficulty of the mathematical problems is *assumed*, not proven. All security will vanish if efficient factoring algorithms are discovered. The second problem is the threat of quantum computers. The theoretical ability of quantum computers to essentially process large amounts of information in parallel would remove the time barrier to factoring large numbers. Thus, public-key encryption, though secure at the moment, faces a serious threat as quantum computing comes closer to reality. Currently, however, this method is still widely used, especially for the encryption of financial information sent over the internet.

Secret-key encryption requires that two users first develop and securely share a secret key, which is a long string of randomly-chosen bits. (Ekert, 1995). The users then use the secret key along with public algorithms to encrypt and decrypt messages. The algorithms are very complex, and can be designed such that every bit of output is dependent on every bit of input (Ford, 2002). Suppose that a key of 128 bits is used. "Assuming that brute force, along with some parallelism, is employed, the encrypted message should be safe: a billion computers doing a billion operations per second would require a trillion years to decrypt it" (Ford, 2002, p.2).

There are two main problems with secret-key encryption. The first problem is that by analyzing the publicly-known encrypting algorithm, it sometimes becomes easier to decrypt the message. This problem can be somewhat offset by increasing the length of the key (Ford, 2002). The second problem is securely distributing the secret key in the first place. This is the well-known "key-distribution problem". Users must either agree on the secret key when they are together in the same location or when they are in different locations. The drawbacks to developing the key when they are in the same location are that it is not always practical for the users to meet, a large database would be needed to store the pre-determined keys, and such storage is not secure. The drawback to developing a key when the users are in different locations is that all classical methods of transmitting the key are subject to eavesdropping that cannot be detected by the users.

Quantum cryptography solves the problems of secret-key cryptography by providing a way for two users who are in different locations to securely establish a secret key *and* to detect if eavesdropping has occurred. In addition, since quantum cryptography does not depend on

difficult mathematical problems for its security, it is not threatened by the development of quantum computers. Quantum cryptography accomplishes these remarkable feats by exploiting the properties of microscopic objects such as photons.

Since photon polarization measurements form the foundation for the most common quantum cryptographic techniques, it is important to first understand their properties. The three chosen bases of polarization and the possible results of a measurement according to the bases are: rectilinear (horizontal or vertical), circular (left-circular or right-circular), and diagonal (45° or 135°) (Ford, 2002). Although there are three bases, only two bases are used in any given protocol for quantum cryptography.

Photons can be measured to determine their orientation relative to one of these bases of polarization at a time. Classically, one would expect the photon to *have* a certain polarization, which can be measured but which is not changed by the measurement. Photons, however, are quantum objects, and in the quantum world an object can be considered to have a property only *after* you have measured it, and the type of measurement impacts the property that you find the object to have. This implies that a photon can only be considered to *have* a particular polarization *after* you measure it, and that the basis you choose for the measurement will have an impact on the polarization that you find the photon to have.

For example, if you send a photon through an apparatus to measure its orientation relative to a rectilinear coordinate system, you are asking the question, "How is the photon oriented relative to a rectilinear coordinate system?" You will find the photon is either vertically polarized or horizontally polarized -- there are only two possibilities. Suppose you measure this photon as horizontally polarized. Next you send this same photon through an apparatus to measure its orientation relative to a diagonal coordinate system. Now you are asking the question, "How is the photon oriented relative to a diagonal coordinate system?", and you will find that the photon is either 45° polarized or 135° polarized – there are only two possibilities. The type of measurement does indeed have an impact on what property you find. This is in surprising contrast to the classical situation where something that is horizontally oriented would be expected to have a component in the diagonal direction . The fact that a horizontally-oriented photon may subsequently be measured to have a 45° polarization occurs because the state of horizontal polarization is actually a superposition of the two diagonal polarization states. All polarization states are actually superpositions of other polarization states.

It is important to note that once the diagonal measurement was made, all information about the previous "property" of horizontal polarization of the photon vanished. As a result it is impossible to determine a photon's rectilinear and diagonal polarizations at the same time. This is analogous to the impossibility of specifying a particle's position and momentum at the same time. More information about one results in less information about the other.

The behavior of photons sent through a series of polarizers is illustrated below:

LEGEND

[+] = an apparatus that measures rectilinear polarization

V = vertical polarization

H = horizontal polarization

[o] = an apparatus that measures circular polarization

L = left-circular polarization

R = right-circular polarization

1. A photon is sent through a rectilinear (+) measurement apparatus. The photon has equal probability of being vertically or horizontally oriented.

photon 1→ [+] → V

photon 2→ [+] → H

2. A photon that is repeatedly sent through the same measurement apparatus will always give the same answer.

photon 1→ [+] → V →[+] → V →[+] → V

photon 2→[+] → H →[+] → H →[+] → H

2. A photon that was measured to be vertically polarized is sent through an apparatus to measure its circular polarization The photon will come out either left-circular polarized OR right-circular polarized, with equal probability.

V →[o] → L OR V →[o] → R

3. Analogous results would occur if a circularly-polarized photon was sent through a rectilinear measurement apparatus.

In 1984, Bennett and Brassard suggested the first protocol, called "BB84," for establishing a secret key using quantum transmissions (Ford, 2002; Ekert, 1995). This protocol uses the rectilinear and circular polarization bases for photons. The steps of the protocol are explained below, using the standard convention that Alice is the sender, Bob is the receiver, and Eve is the eavesdropper.

1. Alice prepares photons randomly with either rectilinear or circular polarizations.

2. Alice records the polarization of each photon and then sends it to Bob.

3. Bob receives each photon and randomly measures its polarization according to the rectilinear or circular basis. He records the measurement type (basis used) and the resulting polarization measured. (It is important to remember that the polarization sent by Alice may not be the same polarization Bob finds if he does not use the same basis as Alice.

4. Bob publicly tells Alice what the measurement types were, but not the results of his measurements.

5. Alice publicly tells Bob which measurements were of the correct type. A correct measurement is the correct type of Bob used the same basis for measurement as Alice did for preparation.

6. Alice and Bob each throw out the data from measurements that were not of the correct type, and convert the remaining data to a string of bits using a convention such as:
left-circular = 0, right-circular = 1
horizontal = 0, vertical = 1

Using an online demonstration program (Henle, 2002), the following example data was generated assuming that Alice sends 12 photons and the detector never fails.

Step	Description	1	2	3	4	5	6	7	8	9	10	11	12
1	Filters used by Alice to prepare photons	+	+	o	+	o	o	o	+	+	+	o	o
2	Polarizations of photons sent by Alice	V	H	L	H	R	L	R	V	H	H	R	L
3a	Measurement types made by Bob	+	+	+	+	o	o	o	o	+	o	o	+
3b	Results of Bob's measurements	V	H	H	H	R	L	R	L	H	L	R	H
4	Bob publicly tells Alice which type of measurement he made on each photon	+	+	+	+	o	o	o	o	+	o	o	+
5	Alice publicly tells Bob which measurements were the correct type	yes	yes	no	yes	yes	yes	yes	no	yes	no	yes	no
6	Alice and Bob each keep the data from correct measurements and convert to binary	1	0		0	1	0	1		0		1	

The string of bits now owned by Alice and Bob is: 1 0 0 1 0 1 0 1. This string of bits forms the secret key. In practice, the number of photons sent and the resulting length of the string of bits would be much greater.

An essentially equivalent protocol that utilizes EPR correlations has been worked on by Artur Ekert and David Mermin (Collins, 1992). To take advantage of EPR correlations, particles are prepared in such a way that they are "entangled". This means that although they may be separated by large distances in space, they are not independent of each other. Suppose the entangled particles are photons. If one of the particles is measured according to the rectilinear basis and found to have a vertical polarization, then the other particle will also be found to have a vertical polarization if it is measured according to the rectilinear basis. If however, the second particle is measured according to the circular basis, it may be found to have either left-circular or right-circular polarization. The steps of the protocol for developing a secret key using EPR correlations of entangled photons are explained below:

1. Alice creates EPR pairs of polarized photons, keeping one particle for herself and sending the other particle of each pair to Bob.

2. Alice randomly measures the polarization of each particle she kept according to the rectilinear or circular basis. She records each measurement type and the polarization measured.

3. Bob randomly measures each particle he received according to the rectilinear or circular basis. He records each measurement type and the polarization measured.

4. Alice and Bob tell each other which measurement types were used, and they keep the data from all particle pairs where they both chose the same measurement type.

5. They convert the remaining data to a string of bits using a convention such as:
   left-circular = 0, right-circular = 1
   horizontal = 0, vertical = 1

One important difference between the BB84 and the EPR methods is that with BB84, the key created by Alice and Bob must be stored classically until it is used. Therefore, although the key was completely secure when it was created, its continued security over time is only as great as the security of its storage. Using the EPR method, Alice and Bob could potentially store the prepared entangled particles and then measure them and create the key just before they were going to use it, eliminating the problem of insecure storage.

But what if Eve has been eavesdropping on Alice and Bob's transmissions? To understand why eavesdropping does not compromise the security of keys developed using quantum cryptography, it is important to note that transmissions between Alice and Bob take place on two different types of channels. The photon transmissions are quantum in nature and occur on what will be called a quantum channel, such as optical fiber. The discussions between Alice and Bob about the *types* of measurements made occur on a classical channel, such as telephone or email. The properties of these two channels are very different.

Eve can intercept information transmitted on the classical channel without being detected. Although this was a serious problem in previous modern cryptographic methods, it is not a problem in quantum cryptography. This is because in quantum cryptography protocols the only information Bob and Alice exchange on a classical channel is the *type* of measurements they made, which tells Eve nothing about the results of the measurement, and therefore nothing about the key that was developed.

Suppose Eve listens on the quantum channel. One way she may do this is by skimming some photons from the burst sent from Alice to Bob. (Although the explanation of the protocol implied that single photons were sent, in practice it is easier to send bursts of photons.) Now Eve has photons that are identical in polarization to those received by Bob, but she has to randomly choose her own measurement type since she doesn't know what measurement type Bob is going to use. Therefore, about half the time she will choose a different basis than Bob for measurement. For example, suppose Alice sends a burst of circularly polarized photons, some of which are received by Eve and Bob. Eve decided to use the rectilinear basis for measurement, and Bob decides to use the circular basis. Alice and Bob keep the resulting data since they both used the same basis, but since Eve used the wrong basis, she doesn't know what their result was. Now suppose instead that Eve had decided to measure it according to the circular basis, but Bob decided to measure it according to the rectilinear basis. Here Eve would know the polarization that Alice sent, but since Bob did not choose the correct basis, Alice and Bob would throw the results out. As you can see, Eve will not end up with anything resembling the string of bits that Alice and Bob create.

Another method Eve could use to eavesdrop on the quantum channel is to intercept the photons, measure them, and then send them on to Bob. When she chooses a different basis for measurement than Alice had used for preparation, she will change the photon's polarization

through the act of measurement, causing Bob to receive a photon that does not have the same polarization as that sent by Alice. For example, consider the following scenario. Alice sends a right-circularly polarized photon, which is intercepted by Eve. Eve measures it according to the rectilinear basis, finds it to be vertically polarized, and sends it on to Bob. Bob measures it according to the circular basis, and has an equal probability of finding it to be right-circularly polarized and left-circularly polarized. It is clear that this will introduce errors into Bob's final string of bits. Alice and Bob can detect these errors when they run a "key validity check", as described below. Thus, although Eve could obtain some correct bits of the final key by intercepting photons, Alice and Bob will know that the security of their key has been compromised.

In the example data generated using the online demonstration program, it was assumed that the detector never fails. In reality, detectors fail some of the time, there is noise in the channel, and Eve could be eavesdropping. All of these factors can cause Bob to end up with a different string of bits than Alice. Thus it is important for Alice and Bob to perform a "key validity check" to confirm that they have the same string of bits. They cannot compare the whole string of bits over a classical channel since this would compromise the security of their key. One approach is to compare a large random subset of their string of bits, assuming that if these match up, then the others that they are not comparing also match up and can be used as the key (Collins, 1992). The bits that they have compared are discarded, since this information was shared over a public channel and could have been intercepted. This technique is useful for detecting eavesdropping, since any activity by Eve would introduce a large number of errors. Another technique was developed by Bennett, Brassard and Jean-Marc Robert of the University of Quebec at Rimouski (Collins, 1992). Using this technique, Alice and Bob agree on certain blocks of bits of their key and calculate and compare the parity of each block. If an odd-number of errors exist, the parity calculated by Alice and Bob will be different. Alice and Bob check many overlapping blocks, and make smaller and smaller block sizes to find the errors. Each time a comparison is performed, Alice and Bob discard the last bit in the block. In this way, errors an be eliminated, and Alice and Bob can be sure that they have the same string of bits for use as the key.

The practicalities of performing transmissions on a quantum channel are not as simple as the theory. The light source is usually an LED or laser, and the sender produces a low-intensity

polarized beam that is emitted in short bursts. The polarization of each burst is randomly modulated to either horizontal ,vertical, left-circular, or right-circular before being sent on to the receiver (Ford, 2002). Recently, researchers at the University of California at Santa Barbara have reported that they have found a way to emit single photons. Single photon emission would prevent Eve from skimming off part of a photon burst, making it possible to produce a key that is "secure from the most advanced attacks." (Savani, 2000).

The quantum information in the form of polarized photons may then be sent over optical fiber or through free space, also called free space optics (FSO) (Bains, 2002). The difficulty with sending quantum information over optical fiber is that polarizations are not retained over long distances (Collins, 1992). Improvements in optical fiber may help extend the distance over which such information can be sent. Another possible way to extend the distances is to use interferometry, looking at differences in phase instead of polarization (Collins, 1992). Using fiber optic cables, photon bits have successfully been transmitted over distances up to 60 km, which is about 37 miles (HP, 2001). Transmitting through the air eliminates the problems of impurities in optical fiber, but so far, successful transmission has been over shorter distances and the weather conditions must be ideal. In early 2002, researchers exchanged a key at night from the mountaintops at Zugspitze and Karwendelspitze in Germany. This transmission over 23.4 km was a record (Bains, 2002). Los Alamos National laboratory has reported an exchange over 1.6 km during daylight (Bains, 2002). Such transmissions could be useful in military applications, where the key is exchanged from one ground station to a satellite and then to another ground station (Bains, 2002).

Whether quantum cryptography will replace classical cryptography techniques will depend on many factors including transmission distance, expense, and ease of use. It is suspected that quantum cryptography is already being used between the White House and the Pentagon (HP,2001; Metz, 2002). There may also be connections between certain military cites, large defense contractors, and research laboratories that are not very far apart (HP, 2001). A possible commercial application that could utilize quantum cryptography is "two-party secure computation" in which two parties compare results of a computation without revealing the data used by each party to complete the computation (Collins, 1992). Since the two parties could be sitting at the same table, distance is not a problem.

In conclusion, the ultimate security of quantum cryptography makes these techniques a valuable resource for this dangerous age when secure transmission of sensitive information is more important than ever.

References

Bains, S. 2002. It's free-space optics' turn. Electronic Engineering Times, March 18, 2002, www.eet.com.

Collins, G. 1992. Quantum cryptography defies eavesdropping. *Physics Today*, November 1992, pp. 21-23.

Ekert, A. 1995. What is quantum cryptography. http://www.qubit.org/index.html Accessed 12/7/02.

Ford, J. Quantum cryptography tutorial. http://www.cs.dartmouth.edu/~jford/crypto.html. Accessed on 11/3/02.

Henle, F. 2002. BB84 Demo. http://www.cs.dartmouth.edu/~henle/Quantum/cgi-bin/Q2.cgi. Accessed on 11/9/02.

Hewlett Packard, 2001. http://searchhp.techtarget.com/sDefinition/0,,sid6_gci284012,00.html. Accessed on 11/27/02.

Metz, C. 2002, Total Lockdown. *PC Magazine*, September 17, 2002. www.pcmag.com.

Savani, J. 2000. Eavesdroppers beware: Single photon emission prepares way for quantum cryptography. UCSB College of Engineering Press Release. http://www.engineering.ucsb.edu/Announce/quantum_cryptography.html.