

Running head: QUANTUM CRYPTOGRAPHY

Quantum Cryptography Revealed

Gary Rogers

Utah Valley State College

ENGL 2020

Brent Baum

4/24/2006

ABSTRACT

The science of cryptography has existed in one form or another for centuries. There are many common implementations of cryptography in use today such as the HTTPS protocol on the Internet. All forms of data encryption and cryptography require a key in some form or another for use in encoding and decoding data. The inherent problem with any form of cryptography is the possibility that the key may be intercepted by an eavesdropper. In a recent breakthrough a technique called quantum cryptography has been shown to possibly guarantee the privacy of an encryption key during distribution using quantum mechanics. As quantum cryptography continues to evolve, it has potential to become the de facto standard for the transportation of confidential information.

1092 West 420 North
Orem, UT 84057

4/24/2006

Brent Baum
ENGL 2020
Utah Valley State College
800 West University Parkway
Orem, UT 84058

Dear Brent Baum:

I hereby submit the following paper titled "Quantum Cryptography Revealed." It fulfills the requirements for my final research paper in ENGL 2020-603.

This paper first explores a brief history of cryptography and encryption methods. These include the German Enigma machine of World War II, as well as the one-time pad used to protect the American Telegraph system. A small presentation of quantum mechanics is then included. With the foundations in place, the paper then covers the modern technology of Quantum Cryptography. Such technology is a revolutionary way to guarantee the privacy on encrypted messages. The methodology of the technology is presented, as well as some pros and cons of its use. I am certain you will find the paper very informative.

Sincerely,

Gary Rogers
ENGL 2020-603

Attachment

Table of Contents

Quantum Cryptography Revealed.....	i
Table of Contents.....	iii
Glossary of Terms.....	iv
Executive Summary.....	v
General Information: Thesis, Audience, Purpose, Organization	vi
Crypto-what?.....	1
A telegram of epic proportions	3
Holy uncertainty Batman!.....	4
A quantum leap.....	5
1984.....	6
Fit for the Guinness Book.....	8
Don't Count Your Chickens	8
To Be Or Not To Be.....	9
Appendix A.....	10
Appendix B.....	11
References.....	12

Glossary of Terms

Alphanumeric	A character that is either a letter of the English alphabet or of the base 10 number system. (I.E. 'a' or '42').
Cryptanalyst	One who analyzes cryptographic methods or ciphertext as a means to understand it.
Cryptography	The Greek roots of this word crypto-graphy mean "secret writing". It is a term used to describe text that has been intentionally altered as a means to protect its privacy.
Polarized light	A focused wave of light that has consistent and measurable wave patterns. There are several classes of polarized light waves such as linear, circular, and elliptical.
Protocol	In terms of Computer Science, it is a set of rules by which data transmission adheres. It allows for both the transmitter and receiver to make sense of one another's messages. There is typically a separate protocol for each type of data transmission. (I.E. Ethernet, PPPoE, BB84, etc.)

Executive Summary

The science of cryptography has existed in one form or another for centuries.

Cryptography is the art of encoding and decoding messages for transmission between two parties, while keeping the message secret from unwanted viewers. There are many common implementations of cryptography in use today such as the HTTPS protocol on the Internet. All forms of data encryption and cryptography require a key in some form or another for use in encoding and decoding data. There are even some modern methods of encryption that have been mathematically proven to be unbreakable if they are implemented properly.

The inherent problem with any form of cryptography is in the method of key distribution. To date, all forms of message encryption have possessed this major vulnerability. As such, it makes no difference whether a secret message is sent via homing pigeon, a radio transmission, a penciled message on a notepad, or whispering to another, there is no physical way to get a cryptographic key to another without running the risk of the key being intercepted.

To solve this dilemma, a radical solution has been proposed called quantum cryptography. This method essentially uses photon light particles to send a key to an intended recipient. The difference with this method of key distribution is that it implements quantum mechanic's uncertainty principle as a means to guarantee the privacy of a key during distribution. Practically, quantum cryptography has the ability to afford complete privacy during the entire broadcast of an encoded message.

Because this technology has simply not existed to date, it presents an extremely beneficial opportunity. As quantum cryptography continues to evolve, it has potential to become the de facto standard for the transportation of confidential information.

General Information: Thesis, Audience, Purpose, Organization

Thesis Statement

A recent breakthrough has occurred within the field of information technology. This breakthrough is known as quantum cryptography. The technology affords the ability to transmit a private key for use in data encryption and guarantee its privacy. As the world has never known the ability to communicate with absolute secrecy, quantum cryptography presents some very intriguing possibilities.

Report Audience

The audience for this research paper are primarily people with an interest in various computer fields such as computer science, information technology, information systems, etc., as well as Brant Baum, instructor of ENGL 2020.

Author's Purpose

The purpose of this research paper is to inform the intended audience about the exciting discoveries and developments within the topic of quantum cryptography

Plan of Organization and Development

This research paper was organized through a multi-step process. The information contained herein was compiled by collecting and summarizing general topical information. The paper was organized in such a manner that the thesis is derived naturally from the stated premises.

Crypto-what?

The science of cryptography has existed in one form or another for centuries. Breaking the word cryptography into its roots crypto-graphy yields the meaning “secret writings.” Cryptography is the art of encoding and decoding messages for transmission between two parties, while keeping the message secret from unwanted viewers. A modern example of cryptography was that of the German enigma machine. This World War II era machine was used to translate battlefield messages and commands into a secret code. These encoded messages could then be distributed by letter, radio, or even Morse code out in the open. Once received by the other party, their corresponding enigma machine could be used to decode the message.

More recently, many may recall during their childhood using the simplest form of encryption to pass secret notes to one another. This method was that of taking each letter in a sentence and increasing its alphabetic value by a constant number. For example, if you had the sentence “mary had a little lamb” and you wanted to encode it through increasing each value by one letter of the alphabet (i.e. $a + 1 = b$, $b + 1 = c$, etc.), you would come up with “nbsz ibe b mjuumf mbnc” (See Appendix A for further detail). In this case, the constant alphabetic offset value (i.e. 1) is referred to as the cryptographic key. All forms of data encryption need a key in some form or another for use in encoding and decoding the data. In our message, the encoded sentence is known as cipher text, or an encrypted message. To make sense of the cipher text, the key is needed to then decode, or decipher the message. However, this method of encryption is extremely weak. As one author notes, “this technique creates a ciphertext that is unintelligible to the casual reader but easily decodable by anyone who knows the trick” (Mullins, 2002).

Today, the most widely used encryption method is Secure Sockets Layer (SSL) or HTTPS on the Internet. Many users are probably familiar with seeing a “gold lock” in the corner

of their browser when making an online purchase or submitting personal data. This “lock” usually means that an encrypted method of communicating with the remote server has been established. However, many have no idea how this method of cryptography functions at the most basic level. Essentially SSL works the same as any other traditional form of encryption. The server and client (the browser) exchange cryptographic keys with each other prior to establishing the secure channel. Once the keys are received, both the server and the browser can begin encoding their transmissions in a form which the other can decode. However, the encoded messages passing between the two machines will be useless to anyone who has tapped the line or who does not have the key which were previously exchanged. What many do not realize is that the first step in establishing the secure channel, the key distribution, is done in a non-secure manner. Because the keys are exchanged between the server and client in unencrypted plain text (non-cipher text), it opens the door for a possible attack (Weaver, 2006).

The inherent problem with SSL, as well as all the previous examples of encryption, is in the key distribution. For instance, the Nazis of World War II regularly broadcasted their enigma keys to commanders at the beginning of each day in battle. The allies obtained a significant advantage in the war when this method of key distribution was discovered. This allowed for enemy messages to be decoded and lead to tactical superiority on the battlefield. To date, all forms of encryption have possessed this major vulnerability. Therefore, it makes no difference whether a secret message is sent via homing pigeon, a radio transmission, a penciled message on a notepad, or whispering to another, there is no physical way to get a cryptographic key to another without running the risk of the key being intercepted. Should an unwanted guest learn the key or code, they would be able to interpret future messages encoded with the stolen key.

A telegram of epic proportions

Although still defenseless to key distribution problems, more advanced methods of encryption make use of increasingly more complex algorithms to generate cipher text. For instance, at the turn of the 20th century the American telegraph system was completely insecure. The system consisted of a complex network of transmission lines running all over the country. Upon these lines were sent simple electric pulses in the form of Morse code. A malicious user needed only the ability to read Morse code and obtain a few inexpensive pieces of equipment to connect, at will, to any telegraph wire and eavesdrop on messages being transmitted. One need only imagine the slew of bank robberies and other such thefts induced by telegraph message interception.

To solve this problem, a clever employee of the US Army Signal Corps named Gilbert Vernam proposed a unique solution. He sought to encode telegraph messages and protect them from eavesdroppers. In doing so, he proposed unique solution, first proposed in 1917 which earned him much acclaim. The Vernam's cipher, which later becoming known as the "one-time pad", was so ingenious, that it has since been mathematically proven as the only encryption algorithm to be unbreakable if properly implemented. Moreover, "if a cryptanalyst has a ciphertext string... encrypted using a random key string which has been used only once, the cryptanalyst can do no better than a guess at the plaintext" (Mullins, 2002).

The following is a very crude example of how one would encode a plain text message with a randomly generated key using Vernam's method (See Appendix B for further detail):

```
Message:      mary had a little lamb
Random Key:   9515650654654687986413
Cipher text:  vfscfmajeefqmqzasnhrene
```

Alphanumeric Lookup:

Space=0, a=1, b=2, c=3, d=4, e=5, f=6, g=7, h=8, i=9, j=10,
 k=11, l=12, m=13, n=14, o=15, p=16, q=17, r=18, s=19, t=20,
 u=21, v=22, w=23, x=24, y=25, z=26.

Therefore, to encrypt the message or generate the cipher text, one can use the following formula. $X + Y = Z$ (if $Z > 26$ then $Z = Z - 27$) where X equals a single alphanumeric lookup value, Y equals the corresponding value of a given position in the random key, and Z equals the encrypted alphanumeric value.

To decrypt cipher text, the following formula can be used. $Z - Y = X$ (if $X < 0$ then $X = X + 27$) where Z equals a single character from the cipher text, Y equals the corresponding value of a given position in the random key, and X equals the decrypted alphanumeric value.

If both the sending and receiving parties have exclusive access to the random private key, both can transmit and receive encrypted messages to one another in absolute secrecy.

Once again, the fundamental problem with Vernam's method was in the means of key distribution. The random key either had to be physically delivered to another telegraph location or quickly transmitted at the beginning of a message before the cipher text. As such, the message security could be easily compromised if an unwanted party were to obtain the key. Thus, it can be concluded that without a secure method of key distribution, any method of encryption cannot be guaranteed. It is in this very area where a flurry of modern research is being conducted. And the solution seems to baffle traditional physical limitations.

Holy uncertainty Batman!

One of the most famous physicists of all-time, Werner Heisenberg, published in 1927 a theory of quantum mechanics dubbed the "uncertainty principle". His research and findings dealt strictly in the sub-atomic realm of physics (e.g., electrons, photons, neutrons, etc). He simply stated that the more finitely one looks to measure a given particle's position, the more

imprecise one's measurement of the same particle's momentum becomes and vice versa. In fact, he states that these two measurements are inversely proportional to one another. More importantly, however, he declared that taking the measurement of a sub-atomic particle inevitably changes one or more of its properties. It may be noted that his research was at times criticized by Einstein and others as to its validity. Consequently, debates within the realm of quantum mechanics still continue today (Wikipedia, 2006).

A quantum leap

While there are some who view Heisenberg's uncertainty principle as a hurdle to overcome problems in various arenas of physics, others have exploited this very phenomenon in some exciting new methods. Enter Quantum cryptography, or more specifically quantum key distribution (QKD). QKD is an ingenious solution to the dilemma of key distribution – the fundamental problem to all encryption methods. In fact, Heisenberg's uncertainty principle is the very crux upon which QKD operates. Consider the following statement:

The genius of quantum cryptography is that it solves the problem of key distribution. This ability comes directly from the way quantum particles such as photons behave in nature and the fact that the information these particles carry can take on this behavior. Sending a message using photons is straightforward since one of their quantum properties, polarization, can be used to represent a 0 or a 1. Each photon therefore carries one bit of quantum information, which physicists call a qubit (Mullins, 2002).

Here, Mullins describes the technique of using polarized light as a means to transmit and receive binary data. The idea of transmitting digital information using waves of the electromagnetic spectrum is nothing new; such technology has been used in satellites and cell phones for years. However, QKD takes this technology to the next level by implementing quantum properties as a means to guarantee the privacy of a message. As you might recall, the problem with traditional

encryption methods is that keys are vulnerable to theft or eavesdropping during their transportation from sender to receiver.

Mullins continues to describe QKD by stating, “To receive such a qubit, the recipient must determine the photon’s polarization, a measurement that inevitably alters the photon’s properties. This is bad news for eavesdroppers since the sender and receiver can easily spot the alterations these measurements cause” (Mullins, 2002). Because the sender or receiver could detect the presence of altered qubits by relying on Heisenberg’s uncertainty principle (should an eavesdropper be listening to the communication), this method has the potential to guarantee complete privacy during key exchange.

1984

The first successful attempt of QKD has already been performed and documented in the BB84 protocol. The BB84 protocol is simply a set of rules used to govern the communication between the sender and receiver. It is named after Charles Bennett and Gilles Brassard who first published their findings in 1984. The protocol utilizes four different polarization states: horizontal, vertical, and both +/-45 degree diagonals. These states are then randomly formed into a series of qubits representing a binary 1 or 0. Often, in order to explain various procedures in cryptography the typical characters Alice and Bob are used as placeholders. “In our example, we will have the horizontal and the +45 degree diagonal represent a ‘1’, while the vertical and the -45 degree diagonal will represent a ‘0’... First, Alice sends Bob a random series of qubits, each in one of the four polarization states. In order to determine the polarization of the photons, two types of detectors are used” (Jones, 2002).

Polarization detectors are complicated pieces of equipment that can read the polarization state of the photon.

The first type will correctly detect a horizontal or vertical polarization (detector A), while the second will correctly detect either of the diagonal polarizations (detector B). Only one detector may be used per photon bit, and the detector can only be trusted to correctly determine the two polarizations it was intended for. As an example, if a horizontal photon is detected by detector B, then the polarization state could be read to be either of the diagonal directions, but it will not be correctly detected as a horizontal polarization (Jones, 2002).

Remember however, that by reading the photon's state, its properties are permanently altered.

Therefore, Alice and Bob will implement countermeasures to detect the number of correct qubits each has received. An abnormal amount of errors may indicate the presence of an eavesdropper. This type of intruder would not be able to successfully receive the qubits without unintentionally altering the data.

During the data exchange, Bob in turn selects a random series of detectors to receive the qubits. Because neither Alice nor Bob have a way to determine the detectors the other uses, they echo their random choices in reply.

Each detector can only correctly determine two of the four possible polarizations. Bob has no method of his own to be able to determine which bits were correct. He then must tell Alice the series of detectors he used to retrieve the data, and Alice can respond by letting him know which if his detectors were correct in determining the polarizations. They will then use the correctly detected bits as the cryptographic key in their system (Jones, 2002).

Once the key has been negotiated, a traditional encryption method can be used to transmit the cipher text. If a key were to be transmitted in this manner and coupled with the use of Vernam's cipher, the data exchange could occur in complete and absolute privacy and be theoretically unbreakable.

In short, this protocol provides a method for distributing private keys needed for data encryption using polarized photons. This proven method, albeit unpractical due to its limited range of a few kilometers, gives hope for the future of quantum cryptography as well as a basis for further research.

Fit for the Guinness Book

More recently, and in perhaps one of the most significant events since the advent of the BB84 protocol, researchers at the Los Alamos National Laboratory have made an engineering breakthrough. According to a national press release in February 2006, the scientists were able to achieve a distance world record for QKD. Using industry standard fiber-optic cable, the team was able to successfully transmit and receive cryptographic keys using quantum methods to a world record distance of just over 31 miles! This news illustrates that the technology is becoming more and more reliable as better methods and devices are being implemented. It is clear that commercial and/or governmental implementations of this technology will be coming in the not so distant future (US Fed News Service, 2006).

Don't Count Your Chickens

Research and development in the quantum cryptography field has been underway for nearly three decades. Until recently, its potential for seemingly bullet-proof security has rested on the theory of quantum mechanics, or more specifically Heisenberg's uncertainty principle. However, new research and development is underway which has indicated that it may be possible after all to duplicate sub-atomic particles. In other words, with sophisticated equipment a given photon could be copied, including its direction, position, and speed, with near exact precision (Schewe, 2006). If proven successful, it would effectively turn Heisenberg's theory on its face, have harsh reverberations within the quantum physics community, and have Einstein screaming "I TOLD YOU SO!" from his grave. It could be a significant problem to quantum cryptography because it would prevent the sender and receiver from detecting eavesdroppers. Therefore, this method could reduce quantum cryptography to a security level of at or below current encryption methods.

To Be Or Not To Be

Because of the inherent problems in traditional information security, I find the possibility of guaranteeing cryptographic security a very lucrative opportunity. As we have learned, this technology has simply not existed to date. But in the technology rests its foundation on the hard work and dedication of many such as Vernam, Heisenberg, and others. Therefore, as quantum cryptography continues to evolve, it may become the de facto standard for the transportation of confidential information.

Appendix A

This chart shows the detail of a simple message encryption using a 1 character incremental value for the cryptographic key:

```

-----
|original sentence      | m| a| r| y| | h| a| d| | a| | l| i| t| t| l| e| | l| a| m| b|
-----
|original numeric value|13| 1|18|25| 0| 8| 1| 4| 0| 1| 0|12| 9|20|20|12| 5| 0|12| 1|13| 2|
|cryptographic key     | 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1|
|modified numeric value|14| 2|19|26| 1| 9| 2| 5| 1| 2| 1|13|10|21|21|13| 6| 1|13| 2|14| 3|
-----
|generated cipher text | n| b| s| z| a| i| b| e| a| b| a| m| j| u| u| m| f| a| m| b| n| c|
-----

```

Alphanumeric Lookup:

Space=0, a=1, b=2, c=3, d=4, e=5, f=6, g=7, h=8, i=9, j=10,
k=11, l=12, m=13, n=14, o=15, p=16, q=17, r=18, s=19, t=20,
u=21, v=22, w=23, x=24, y=25, z=26

Appendix B

This chart shows the detail of a complex message encryption using Vernam's cipher to generate a random cryptographic key (notice the difference in the key values to Appendix A):

original sentence	m a r y	h a d	a	l i t t l e	l a m b
original numeric value	13 1 18 25 0 8 1 4 0 1 0 12 9 20 20 12 5 0 12 1 13 2				
cryptographic key	2 3 2 6 9 1 8 2 6 2 6 2 0 1 5 1 2 4 5 1 4 2				
modified numeric value	15 4 20 4 9 9 9 6 6 3 6 14 9 21 25 13 7 4 17 2 17 4				
generated cipher text	o d t d i i i f f c f n i u y m g d q b q d				

Alphanumeric Lookup:

Space=0, a=1, b=2, c=3, d=4, e=5, f=6, g=7, h=8, i=9, j=10,
 k=11, l=12, m=13, n=14, o=15, p=16, q=17, r=18, s=19, t=20,
 u=21, v=22, w=23, x=24, y=25, z=26

References

- Weaver, A (2006). Secure Sockets Layer. *Computer*, 39(4), 88-90.
- BB84.(2005). *IEE Review*, 51(7), 34-34.
- Jones, J. (2002). From Information Technologist to Quantum Specialist.
Brigham Young University.
- Mullins, J., & Moore, S. K. (2002). Making unbreakable code. *IEEE Spectrum*,
39(5), 40.
- Schewe, P., & Stein, B. (2006). Attack of the teleclones. Retrieved February
20, 2006 from
<http://www.aip.org.erl.lib.byu.edu/pnu/2006/split/765-1.html>.
- US Fed News Service, Including US State News (2006). New technologies
enhance quantum cryptography.
- Wikipedia contributors (2006). Uncertainty principle. *Wikipedia, The Free
Encyclopedia*. Retrieved February 26, 2006 from
http://en.wikipedia.org/w/index.php?title=Uncertainty_principle&oldid=41013838.