

---

# Quantum Cryptography

Author: Mark Stacey  
Department of Computer Science  
University of Idaho  
Moscow, Idaho 83843

Attention:  
Tony Shaska  
University of Idaho

**Abstract:**

This report briefly describes the growing study of secure key generation for use by encryption algorithms. With computation power growing so rapidly, a key generation method independent of computational power as well as secure from eavesdropping is required by computer scientists. This has been accomplished through quantum cryptography. Quantum cryptography uses the various properties of light photons and polarizations of those photons to create an entirely new method of key generation. Various beneficial photon characteristics include: random polarization assigned at creation and when cloned; applied Uncertainty Principle signals unwanted tampering and polarization calculations; ability to transport through normal atmosphere; polaroid screen accepting and/or denial of photons. Because quantum cryptography is based upon these properties and not mathematics, encrypted data integrity is maintained for an unlimited time period even when unlimited computing power is available.

Date: May 3, 2005

---

## Table of Contents

<u>Section</u>	<u>Page</u>
Executive Summary.....	3
Forward.....	4
Physical Transportation.....	5
Why Light Photons?.....	6
Measurement of Photons by a Polaroid Screen.....	8
Transportation Protocol.....	11
Key Generation.....	11
Security Obtained.....	13
Conclusion.....	14
References.....	16

Figures and Tables:

Polarization	Constantly Accepted	Randomly Accepted	Constantly Rejected
		\ /	—
—	—	\ /	
/	/	—	\
\	\	—	/

Figure 1. Possible Accept States

## Executive Summary

All computers communicate with other computers, each one sending and receiving data. Much of this data is sensitive to specific parties and needs to be encrypted to maintain integrity. For encryption however, a secret key (series of bits) must be known to the sending and receiving parties while remaining unattainable to the outside world. This creates the dilemma of how two distant parties agree on a shared secret number when the entire world can view all communications.

Quantum cryptography solves this problem by using light photon properties as well as the polarizations of those photons. These properties include: (1) the polarization assignment of each photon upon creation is random; (2) each polarization calculation changes the original state and therefore can be identified.

Quantum cryptography offers many aspects of security: If a third party captures the photons while in transit, calculates the polarization and resends the stream, the receiving party is notified of the tampering. If the photon stream is cloned there is no assurance the cloned polarizations will be equal to the originals. Due to the fact the generated key is not mathematically based, the encrypted data will remain secure no matter the given computational power.

By using this type of key generation two distant parties can generate a secret key to be used by an encryption algorithm. The key generation is secure from tampering due to the photon properties. In the same respect, the final secret key is secure for countless years due to the fact it is not a calculated number and, therefore, cannot be derived by methods known today.

# Quantum Cryptography

## Forward

Computers are constantly sending information back and forth. Much of this data is sensitive, such as bank accounts and government documents. For information security studies, it is assumed every one of these communications is public. Therefore, the sensitive data must first be encrypted using some algorithm before it is sent across a public channel. This way a third party viewing the information while in transit will only see encrypted data rather than the original message.

Currently, almost all encryption algorithms require a secret key. This secret key is simply a series of 1's and 0's that are entered into the encryption algorithm with the data to be encrypted. This key must remain private to both parties of every communication for encryption and decryption.

This presents the question of how two distant parties decide on a shared secret key when all communication is done over what is assumed to be a public channel. In the past and present, this is being done with mathematics and prime number manipulations. However, given the exponential increase of computational power through the past few years, these calculated numbers are becoming more and more susceptible to being cracked and discovered, thus revealing the secret key and, in turn, the original data. This creates the need for further complicated and more intricate mathematics as computation speed and power become more available to the common user. Also, if storage of a certain material needs to be measured in years, this data must be routinely decrypted and re-encrypted using a more recent encryption standard.

The severity of this growing problem has sparked the study for a key generation technique that cannot only offer security measured in years, but is secure from unlimited computational power. Also, during key generation, when we assume anyone can eavesdrop, the ability to determine when someone is “sniffing” the line is imperative. While this may seem impractical, a new system is currently being developed called quantum cryptography which uses not obscure mathematical computation but light photons. Using this procedure, security is based on the laws of physics and photon properties.

In order for this type of key generation to work, we need a method for sending these photons (often generated by a laser) between parties, commonly referred to as Alice and Bob in computer applications, who wish to communicate. It is important to note that Alice and Bob refer to machines and not actual people. Therefore, when transmission is denoted as “Alice to Bob,” consider machine Alice is communicating data to machine Bob. The actual end-users of each machine do not know, nor do they often need to, what is going on between machines at the hardware level.

In this report consideration is given to the physical transportation of the photons from sender to receiver, why light photons were chosen as described by given properties, as well as the protocol methodology used, key generation technique, and security offered through quantum cryptography.

### **Physical Transportation**

Current photon travel commonly uses fiber-optic cable [8:1]. In 2002 a Swiss group of scientists managed to transport a quantum photon stream over 60 kilometers through fiber-optic cable [2:1]. With this distance, communication using quantum cryptography is possible between banks, government buildings, and any other secure communication in a relatively small city.

The method of atmosphere transmission involves sending the light particles from one source to another through the normal air that surrounds us. This would eliminate the necessary physical connection for transactions. In 2000 the Los Alamos National Laboratory was able to send and receive a light particle beam 1.6 kilometers through normal air [2:1]. Recently, British researchers have claimed to send and accept a stream through 23 kilometers. While this is far from the underlying goal of secure communication to LEO satellites 1000 kilometers away, the distances obtained are growing [2:1].

It is important to note through-air transmission is being tested at our atmosphere level where ambient light is the greatest and atmosphere impurities are high, such as smog, fumes, and pollution [4:1]. Once the photons begin leaving our atmosphere toward space satellites where the interference is negligible, travel should become much easier. Scientists believe 1.6 kilometers through common air is comparable to the travel from sealevel, through our thinning atmosphere, to space [4:2]. It is currently unknown when this secure satellite control will be possible.

### **Why Light Photons?**

Light can be considered as a wave or, in this case, a self-contained particle [4:1]. Thus a stream of light can be thought of as a stream of particles, like bullets from a gun rather than water from a hose. This anomaly allows scientists to consider light made up of “wavicles” [4:2]. This knowledge is necessary for considering the light particles as actual “information particles” in this instance.

Photons were also chosen for this type of cryptography due to their truly random nature. Once a photon is created, the properties, such as polarization, are assigned by a truly random style [3:3]. It is important to note that unlike any computed number, this quality is perfectly random, and there is no way to predict the outcome with any accuracy.

In association with randomization there is another property of photons that makes cryptography possible, known as the Uncertainty Principle. Professor Werner Heisenberg defined the Uncertainty Principle in an article published in 1927 [3:1]. This principle states that once a photon is examined or measured, its state is altered. For example, when using an electron microscope to examine the properties of photons the measurement is limited by the wave length of light illuminating the electron, known as  $\gamma$ -rays [3:3]. The Uncertainty Principle explains that at the instant when the position of the photon is determined (this is at the instant when the photon is scattered by the electron), the electron has experienced recoil disturbing its momentum. The photon suffers the same effect and, therefore, its properties have been modified, thus the momentum cannot be accurately measured [3:3].

Heisenberg also stated the smaller light wave employed, the greater the displacement. In other words, the more exact the position is measured, the less precisely the momentum is calculated as this property will be displaced by the degree of the light wave used [3:3]. Essentially, we cannot measure photon properties without displacing their state, even if only by a fraction of a degree. Therefore, we can determine a photon has been measured by a party not present during the measurement.

The next advantage is the polarization of photon particles. When a particle travels, it has a vibration of some axis. This is referred to as the photon's polarization. Normal light has no common polarization; the photons are generated with true randomization, as stated above, and therefore each has random polarized properties [10:1]. Therefore, the light beam contains photons each vibrating in their own sequence.

For general purposes, the varied qualities of this polarized position are described by: 1. A rectilinear polarization consisting of either vertical “|” or horizontal “–” vibration. 2. A diagonal polarization is described as a left diagonal “\” or a right diagonal “/” vibration. 3. A circular polarization is a particle moving in a corkscrew motion as it travels through space, either clockwise (right oriented), or counterclockwise (left oriented) [11:1]. For most implementations

currently in use, only rectilinear and diagonal polarizations are used. Studies are being done involving the circular motions as well. These studies are completed using a rotating magnetic field and are known as “six-state” due to the possible six states of the vibrations [6:2]. For simplicity, however, this paper will only involve the generic four state possibilities “|, —, \, /.”

### Measurement of Photons by a Polaroid Screen

The photons must first be passed through a “polaroid screen” to obtain some known factor of these vibrations [10:1]. A polaroid screen in this context is used to set the polarization to a constant state. If the photon is then sent to another polaroid screen, the screen may or may not allow the photon to pass through. A polaroid screen acts as a filter, allowing some polarizations to pass through while not allowing passage to other polarizations. It is easy to think of a polaroid screen as a paper with a directional slit in it. The slit has four possible directions, each equal to a possible polarization. As a further example, consider a coin slot; it seems logical a vertical coin slot will allow the passage to a vertical coin while not allowing a horizontal coin to pass.

Based on this idea, it is important to note that for every polarized photon there is an equivalent polaroid screen that will allow passage to the photon, an opposite polaroid screen that will deny the photon, and two that give no constant result.

<u>Polarization</u>	<u>Constantly Accepted</u>	<u>Randomly Accepted</u>	<u>Constantly Rejected</u>
		\ /	—
—	—	\ /	
/	/	—	\
\	\	—	/

Figure 1. Possible Accept States

It has been verified that a vertical polarized photon will pass through a “|” polaroid screen and be rejected passage through a horizontal “–” screen. The same is true for diagonal polarization; a left diagonal “\” vibrating photon will pass through a left diagonal screen and be rejected by a right diagonal “/” screen and vice versa [12:3]. So, when a photon enters a screen, it must be either completely accepted or completely rejected. It is not possible to split the photon into smaller units of energy allowing some to pass and some to not [9:3]. Consider a single quantum event that creates a pair of photons. Conservation laws require a correlation of properties like polarization for the pair. Thus, the probability that both will pass through the same pair of polaroid screens is  $\cos(\theta)$  where  $\theta$  is the angle between the screens. If the first screen is horizontal and the second is vertical, the  $\theta$  between them is  $90^0$ . We can see here that the  $\cos(90^0) = 0$ , thus the probability that both photons will pass through both polaroid screens is 0 [9:3]. This should seem implied by what we now know of polaroid screens; we can filter out light with a certain polarization by using perpendicular polaroid screens.

However, there is a catch. It is possible for a rectilinear polarized photon to pass through either of the diagonal screens. It is perfectly random whether this is allowed or denied. The Uncertainty Principle applies to this informality by demonstrating that once the polarization is calculated (whether or not it is allowed to pass through the screen) the photon property of polarization has changed [12:3]. This is easily described by stating once a photon has passed through a screen, the photon adapts the polarization of that screen. For instance, if a “|” photon is rejected by a “\” screen, the polarization remains “|.” However, if the photon is allowed to pass, the polarization is changed and is now “\” [12:3]. If the same photon is then sent to a “|” screen, whether or not the photon will be allowed to pass is perfectly random. Therefore, we are not certain if the polarization of the photon’s original state was measured correctly.

To further explain this, resort to the previous example of two screens with a phase difference of  $90^\circ$ . If we insert a third screen set at a  $45^\circ$  angle in the middle of the two, this creates a phase difference of  $45^\circ$  between the first and second screen. We can then see the probability the photon will pass through the second screen by  $\cos(45^\circ) = \frac{1}{\sqrt{2}}$ . Assuming the photon is then allowed to pass through the third screen, the value becomes  $\cos(45^\circ)^2 = \frac{1}{2}$  [9:1]. This demonstrates that on average half of the photons sent will make it through all of the screens. This is, however, only a mathematical estimation. By this calculation it would seem that the second polarizer changes the angle of polarization of the photon. Otherwise, nothing would make it through the last screen [9:1]. Given this information, we cannot correctly measure the polarization without already knowing something about the photon.

At first, the Uncertainty Principle seems to present a problem when using polarizing screens to calculate the photons. However, this is one of the many features making quantum cryptography secure.

*\*Note\** Quantum cryptography has been an item of study and implementation for almost ten years. Due to this, several various protocols as well as complete systems have been introduced and implemented. This section will cover a very simple generic protocol for describing the methodology behind quantum cryptography. Therefore, it is important to understand the protocol and key generation technique described below are simply used to present a base understanding of the idea behind quantum cryptography.

## Transportation Protocol

Beginning with machine Alice wishing to communicate securely with machine Bob, Alice creates a designated number of photons by using an optical laser capable of emitting individual photons. For this example, consider Alice generating 2000, then sending them to Bob at some designated time interval. This is done because some degree of photons is lost during transition to atmosphere impurities or refraction of ambient light and to ensure Bob knows which photons he received [8:2]. For instance, if Alice sends a photon every  $1/32$  of a second, Bob knows if he received a photon, then waited for  $2/32$  of a second before receiving the next, the middle-sent photon was missed. In this instance, Bob tells Alice which photons he missed and both parties discard those photons. Bob then records the number and sequence of received photons.

At this point, Alice has sent the photons to Bob who has received some percentage of them. This percentage is known and used to generate the private key.

## Key Generation

Before the photons are sent by Alice, they are polarized individually by using a random sequence of polaroid screens. For each set of polarizations (rectilinear and diagonal) Alice assigns one of each to a binary number [1:2]. Under this system, consider Alice as using “|” and “\” as representing a 1, while “—” and “/” represent a 0. This information is made clear to Bob as well. At this point Alice has sent to Bob a 2000-long string of randomly polarized photons.

As the photons approach, Bob waits to test each with one of two polaroid screens. Bob may only use one of each set of polaroid screens; one must be rectilinear “|” or “—” while the other must be diagonal “\” or “/.” It does not matter the order of polaroid screens used by Bob

when receiving the photons. This, in fact, should be as random as possible as well as private only to Bob [1:3]. Continuing the previous example, consider Bob as choosing the vertical “|” and right diagonal “/” screen.

Bob then records the acceptance of the photons as well as which polaroid screen he used to test each photon. Once all photons are received and calculated, Bob and Alice each have a 2000-long string of 1’s and 0’s (called bits), the polaroid screen used associated with each bit, and whether or not the photon was allowed passage through the screen.

At this point Alice and Bob are able to communicate, over what is considered to be a public channel, about which polaroid screen they used to test each photon. During this communication, they only state whether they used a rectilinear or diagonal screen; knowledge of what specific filters were used by Bob should remain private to only Bob. For photons where Bob and Alice used the same type of screen, they have the same bit. For photons where Alice and Bob used different screens, they are not assured they have the same bit and therefore discard it [1:3].

For instance if Alice sent Bob a vertical photon “|” and Bob tests it with a vertical screen “|,” he knows both Alice and he used a rectilinear filter, the bit was accepted, and therefore Alice is sending him a 1. If Alice sends him a horizontal photon “–” and Bob tests it using a vertical screen “|,” he knows Alice used the same filter as himself and the bit was rejected; as a result Alice is sending him a 0. However, if Alice sends Bob a right diagonal photon “/” and Bob tests using a vertical screen “|,” Bob cannot be sure whether Alice sent him a 1 or a 0 because there is no certainty whether or not the photon would pass through or be rejected. At this instance Bob and Alice both discard the given bit and continue the comparison.

Because there are four possible polarization states, assuming all photons made it to Bob, 25% of the time Alice and Bob will have chosen the same polaroid screen and, therefore, can be confident they have equivalent bits. This means if 2000 were sent, Alice and Bob will have 500

analogous bits. If the key needs to be a certain length, the two parties are able to simply discard the amount of unnecessary bits off the end [4:2].

At this point, Alice and Bob both have an identical, designated length bit string. This is the secret key used for their encryption. Because they both have the exact same string, they can each use this for encryption and decryption.

## **Security Obtained**

Because all channels are considered to be public in computer science, we must assume an eavesdropper, often called Eve, can see and intercept all data sent between parties Alice and Bob. Such an instance where Eve is present during a transaction is considered a “man in the middle” attack. Quantum cryptography protects us from this attack in several instances.

First of all, let us assume Eve has intercepted every photon sent to Bob, tests it using a random sequence of polaroid screens (if Eve is smart, she will choose one of each set of polarizations such as Bob does), and then sends them on to Bob. It is possible for Eve to do this quickly and at some time interval for each one, thus offering no detection in the sequence or time period relapse of each photon sent to Bob. Such action will be detected by Bob because of the Uncertainty Principle [4:4]. Obviously, part of the time Eve will have used a diagonal screen when she should have used a rectilinear. When this happens and the photon is accepted, the polarization of that photon has changed.

Such attacks are tested once both parties, Alice and Bob, have the 500 long equivalent bit strings by simply comparing some percentage of the bits openly. Often this percentage is 25% or less and thus does not threaten the entire key’s integrity. In this example Bob and Alice would randomly choose 175 bits of the 500 to compare [4:4]. If any one of the bits is not the same to Alice and Bob, they know there has been some calculation of the bits by a third party. When such tampering takes place, the entire project is discarded and started over [6:2]. While this may

seem time consuming, a new key is computed for every new transaction and, therefore, the protocol is designed to be executed very quickly. For example, consider how many bank transactions are handled a day, then consider for required security a new key needs to be generated for every transaction.

Current quantum cryptography systems move data at a rate of 1000 bits per second. While this is slow compared to current data transition (actually this is a mere 1/10,000 the speed of current data speed), the rate is expected to increase substantially as laser photon transmitter and receptor technology increases [8:2].

To avoid this, Eve may intercept all photons sent to Bob, clone them, and then resend them to Bob. By doing this Eve could wait to test the photons until Bob has tested the photons, hear the order of screens with which Bob calculated the photons, and then test the cloned photons using the same order of screens [4:4]. However, this will also not work for Eve because one of the properties of photons is that once created, the polarization is perfectly random. This includes when cloning. Because there are four possible polarization states, Eve's cloned photons will each have a 25% chance of being equal to the original. Furthermore, Eve does not know what two screens Bob will use as well as the sequence (this is why Bob must choose the order of polaroid screens randomly) [4:5]. Given these percentages, there is no possible way Eve's generated key will be equivalent to that of Bob and Alice.

## **Conclusion**

Due to growing encryption needs as well as computational power increasing exponentially, data integrity is being threatened. Due to this, a secret key generation method secure from known attacks offering high data integrity measured in years and decades is needed by computer scientists. This has been accomplished through quantum cryptography. Using light

photons, security is gained from the fact the secret key is not a calculated number, but generated by photon polarizations. This means that while a mathematically calculated secret key will eventually be broken as computer speed and power increases, a quantum cryptography key will be indefinitely secure. This enables the security of encrypted sensitive data for countless years [6:5]. Government documents, for example, will no longer need to be decrypted and then encrypted again using new techniques as new encryption standards arise and old ones become obsolete.

## References

1. Metz, Cade. (2002, Aug. 6). "Quantum Cryptography Arrives: Going for the Unbreakable." PC Magazine, pp. 17-24.
2. Duncan Graham-Rowe. (2002, Oct. 2). "Quantum Cryptography Takes to the Skies." New Scientist, Vol. 419, pp. 450.
3. Hilgevoord, Jan, Uffink, Jos, "The Uncertainty Principle", The Stanford Encyclopedia of Philosophy (Winter 2001 Edition), Edward N. Zalta (ed.),  
<<http://plato.stanford.edu/archives/win2001/entries/qt-uncertainty/>>.
4. Dejesus, Edmund X. (2001, Aug.). "Quantum Leap." Information Security, pp. 35-47.
5. Enzer, Daphna G., Hadley, Phillip G., Hughes, Richard J., Peterson, Charles G., Kwiat, Paul G. (2002, July 12). "Six-State Protocol Offers Advantages for Quantum Cryptography." Institute of Physics: New Journal of Physics Quantum Cryptography Focus Issue 4, Vol. 57. pp. 45.1-45.8.
6. Ford, James. (2003, Dec.). "Quantum Cryptography Tutorial".  
<<http://www.cs.dartmouth.edu/~jford/crypto.html>>.
7. Bieber, Celeste. (2004, June 4). "First Quantum Cryptography Network Unveiled" New Scientist, Vol. 756, pp. 23.
8. Saltever, Alex. (2003, July 15). "A Quantum Leap in Cryptography". Business Week Online.  
<[http://www.businessweek.com/technology/content/jul2003/tc20030715\\_5818\\_tc047.htm](http://www.businessweek.com/technology/content/jul2003/tc20030715_5818_tc047.htm)>.
9. Paul P. Budnik Jr. (2003). "Polarized Light". Mountain Math Software.  
<<http://www.mtnmath.com/whatrh/node78.html>>.
10. (2004). "Polarized Light". "MSN Encarta".  
<[http://encarta.msn.com/media\\_461531346\\_761576625\\_-1\\_1/Polarized\\_Light.html](http://encarta.msn.com/media_461531346_761576625_-1_1/Polarized_Light.html)>.
11. (2004). "Polarization". BrainyEncyclopedia.  
<<http://www.brainyencyclopedia.com/encyclopedia/p/po/polarization.html>>.
12. Czachor, Marek. (2003, Nov. 12). "Quantum Cryptography with Polarizing Interferometers".  
<<http://ernie.ecs.soton.ac.uk/opcit/cgi-bin/pdf?id=oai%3AarXiv.org%3Aquant-ph%2F9812030>>.