# Cryptography: Mathematical Advancements on Cyber Security

Kristin Bower

A Senior Thesis submitted in partial fulfillment
of the requirements for graduation
in the Honors Program
Liberty University
Spring 2019

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial fulfillment of the requirements for graduation from the Honors Program of Liberty University.

_____

Scott Long, Ph.D.
Thesis Chair

_____

Daniel Joseph, Ph.D.
Committee Member

_____

Melesa Poole, Ph.D.
Committee Member

_____

Mark Ray Schmidt, Ph.D.
Assistant Honors Director

_____

Date

## Abstract

The origin of cryptography, the study of encoding and decoding messages, dates back to ancient times around 1900 BC. The ancient Egyptians enlisted the use of basic encryption techniques to conceal personal information. Eventually, the realm of cryptography grew to include the concealment of more important information, and cryptography quickly became the backbone of cyber security. Many companies today use encryption to protect online data, and the government even uses encryption to conceal confidential information. Mathematics played a huge role in advancing the methods of cryptography. By looking at the math behind the most basic methods to the newest methods of cryptography, one can learn how cryptography has advanced and will continue to advance.

# Cryptography: Mathematical Advancements on Cyber Security

How does the government keep its secrets from prying eyes? How do companies who promise to keep their customers' personal information safe actually protect that information? In most cases, the answer is cryptography, the study of encoding and decoding information. Starting with rudimentary beginnings, cryptography evolved to include complex mathematical techniques. As mathematicians discovered new aspects of prime numbers and functions with unique properties, the government updated the standard practice for encoding and decoding information in order to keep up with the growing field of mathematics. Still today, researchers seek for new methods to add to cryptography, and as mathematics continues to advance so will the area of cyber security.

## History of Cryptography

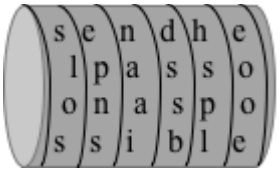
Cryptography, the study of encryption and decryption, stems from the basic desire for privacy. The most basic examples of the encryption and decryption process, though rudimentary compared to modern methods, involve the concept of sending information to a location without interception from an unintended source. The first known instance of cryptography occurred around 1900 BC in ancient Egypt. The tomb of Khnumhotep II, an Egyptian nobleman, contains several hieroglyphic symbols. However, the last sections of the hieroglyphics include abnormal symbols replacing the usual symbols (Dooley, 2018). The unusual symbols obscure the meaning of the hieroglyphics by simply switching commonly used symbols with unknown symbols. Though simple in nature, the act of switching symbols to conceal a message is a basic form of encryption. Nonetheless, one cannot determine with absolute certainty why Khnumhotep II hides the true meaning of the inscriptions, so the reasoning behind the ambiguity remains unclear.

Assyrian merchants during 1500 BC introduced the idea of using intaglios for business transactions. An intaglio, an engraved figure in a stone or other hard material, allowed the merchants to create a unique signature, which ensures that trading occurs with the intended merchant (Dooley, 2018). The idea of using a unique signature foretells the idea of digital signatures, a more mathematically complex way to ensure the authenticity of a transaction.

Meanwhile, during the 7th century BC, a Greek poet named Archilochus introduced the skytale, a cryptographic device consisting of a cylinder with a leather strip (Dooley, 2018). Suppose the skytale allows for four letters written around the cylinder and six letters written along the side, then skytale encrypts messages as follows:

**Step 1**. Create the message: “Send help as soon as possible”

**Step 2**. Write message along the side of the cylinder like the example below.




**Step 3**. Unwrap the leather strips to obtain the new encrypted message: “

slosepnsnaaidssbhspleooe ”

Notice: In order to decrypt the message, one must simply rewrap the leather strip around the cylinder and read along the side. This method obviously presents several limitations regarding the length of the original message and the ease of deciphering the encrypted message but proves effective for the time period of the skytale’s use.

One of the most famous examples of early cryptography, the Caesar cipher, emerged around 100 BC. Julius Caesar developed a shift cipher known as the Caesar

cipher in order to protect confidential military information (Dooley, 2018). The cipher takes the letters used in the message and shifts each letter of over three to the left, or 23 to the right, according to the order of the alphabet. For example, if one wants to encrypt the message "WE LEAVE AT SUNDOWN", then by using the Caesar, he obtains the following:

**Original Message:** WE LEAVE AT SUNDOWN

**Encrypted Message:** TB IBXSB XQ PRKALTK

**Innovations to Cryptography**

The ancient examples of cryptography certainly paved the way for more advanced cryptographical techniques; however, several basic developments still needed improvement. Even though the encryption techniques introduced thus far concealed information, one could easily decrypt the message without much effort. In order to further protect hidden messages, cryptographic techniques needed more complexity.

Leon Battista Alberti, an Italian Renaissance man, created the first polyalphabetic cipher, known as the Alberti cipher, around 1467. The Alberti cipher involves two concentric disks, one larger and one smaller, each divided into 24 sections. The stationary larger disk contains the uppercase letters of the Latin alphabet, which consists of the English alphabet minus J, U and W. In addition, Alberti also took out the letters H, K and Y as he personally regarded them unnecessary, and he added the numbers 1 through 4 to the outer disk, as well. The inner disk consists of the lowercase letters of the Latin alphabet, which also disregards j, u and w from the English alphabet, and also contains the symbol et, which most likely carries the meaning of the '&' symbol (Dooley, 2018).

In order to encode a message, one must simply rotate the inner disk and replace the letter or number on the outer disk with the letter directly underneath on the inner disk.

As encryption and decryption techniques advanced, these methods began to spread, especially with the invention of the printing press. Johannes Trithemius published posthumously the first printed work on cryptography in 1518. His work entitled *Polygraphia* is a composition of five books (Dooley, 2018). The books contain ancient alphabets, invented alphabets, and examples of encoding messages. The printing of cryptographical works allowed encryption and decryption techniques to spread farther than ever before.

As the interest in creating cryptosystems grew, the interest in defeating cryptosystems also emerged. Thus, the birth of cryptanalysis, the science of breaking cryptographic algorithms, occurred during the 19$^{th}$ century. Edgar Allen Poe, the famous American poet, showcased his skills in a Pennsylvania paper by solving submitted ciphers. Poe's efforts to break encryptions spread the interest of cracking encryption techniques for entertainment. However, the increased interest in cryptanalysis pushed the need for stronger encryption techniques (Dooley, 2018).

Eventually, governments also began to pay attention to cryptanalysis. During World War I, the cryptanalysis section of the British Naval Intelligence decrypted about 15,000 German messages. This allowed the British Navy to play an important role in defeating Germany during WWI. The realm of cryptography, now not only involved methods for hiding important messages, but also involved the practice of breaking encrypted messages. The ability to decrypt encoded messages allows one to gain an advantage over enemies without their knowledge (Budiansky, 2016).

## Modern Advancements

As the interest in cryptography grew, the need for more complex methods also arose. Thus, cryptographers sought to incorporate more difficult mathematical tactics in order to protect their encryption techniques from adversaries (Middleton, 2017). Whitfield Diffie and Martin Hellman, two prominent cryptographers of the 20th century, incorporated the use of prime numbers into their encryption method, utilizing the difficulty of factoring large prime numbers (Mollin, 2003). Diffie and Hellman created a method to exchange keys, vital information used in encoding and decoding, called the Diffie-Hellman key exchange. Essentially, the Diffie-Hellman key exchange involves the use of a public key, which is a prime number known by the general public, a nonzero integer agreed upon by the two parties exchanging information, and a unique secret key for each of the two parties. Surprisingly, when using the Diffie-Hellman key exchange, each party does not need to know the secret key of the other party in order perform the required calculations. The specifications of the key exchange will be discussed later in detail.

The 20th century also introduced the first commercially established cipher, known by the name Lucifer. With the formation of the National Security Agency (NSA) during 1952, the American government began to search for more ways to ensure the protection of domestic information (Yan, 2008). Several workers of the IBM, or International Business Machines Corporation, created Lucifer and submitted the cipher to the NSA as a possibility for the Data Encryption Standard (DES). After acceptance from the NSA, Lucifer served as the basis for the DES, which became the government standard for encryption (Yan, 2008).

Although the discovery of a special curve, known as the elliptic curve, dates back to the 18th century, the widespread implementation of elliptic curves into cryptography did not occur until the beginning of the 21st century. The unique properties of addition over an elliptic curve add important applications to cryptography. Elliptic curve cryptography also enables more security with a smaller key size than the Diffie-Hellman key exchange (Washington, 2003). The process of elliptic curve addition seems simple to compute, however given large enough prime numbers the process becomes increasingly more difficult. The NSA even accepted the use of elliptic curve cryptography as a national standard for the encryption of information. However, the NSA announced the plan to replace the use of elliptic curve cryptography with a newer cipher in 2015 due to the impending threat of quantum computing (National Security Agency, 2015).

**The Future of Cryptography**

The unpredictability of the quantum realm makes the idea of quantum cryptography a virtually unbreachable option for encoding important information. The beauty of encoded data within a quantum state is that the moment an outside force tries to intercept or read the encoded data, the data itself changes. Thus, eavesdropping is easily detected the moment of occurrence. Quantum cryptography involves the use of photons and a photon detector. Once the photon contains the hidden message, the photon detector uses the random rotations of the polarization of the photon to transfer the message into bits (Horodecki, 2010).

Since quantum cryptography is practically safe from any interference, it seems completely infallible; yet, several complications make it hard to implement. One problem with quantum cryptography is the short distance limitation for sending the data. An

important aspect of quantum cryptography is the entanglement of photons, the idea that two photons are linked even though there is no physical attachment between the two photons (Horodecki, 2010). However, entanglement can only occur over a relatively short distance. In 2017, scientists in China created a new record for the longest distance for successfully transmitting entangled photons, 1203 kilometers, or approximately 760 miles (Chen, 2017). This distance is an incredible breakthrough, but room for major improvement still exists.

Another area of concern with quantum cryptography is cost. For practical and commercial uses of quantum cryptography, a reasonable cost and availability of the required resources is nonexistent. Since much of quantum cryptography is still in the developmental stages, many of the resources available to scientists and researchers are not available generally. The network and equipment required for the quantum key distribution, as well as the photon detector costs more than a business would typically want to pay to add more security to the company (Sergienko, 2006). Once the accessibility and the cost of the technology associated with quantum cryptography reach a more affordable level, then wide spread implementation of quantum cryptography is inevitable.

## Private and Public Key Cryptography

In order to understand the role of mathematics in cryptography as a whole, one should first attempt to understand how mathematics is used in the individual methods. An important distinction to realize is the difference between private and public key cryptography, but first one must consider the nature of a key itself and its purpose.

A key is a piece of information that enables the sender of a message to encrypt the message and the receiver of a message to decrypt the message (Hoffstein, Pipher, & Silverman, 2008). For example, consider the Caesar cipher mentioned previously. This particular cipher shifts each letter to the right by 23. Thus, the encryption key is 23. However, the decryption key is less obvious than the encryption key in this example. Remember in the previous discussion that shifting each letter of the alphabet to the right by 23 is equivalent to shifting each letter over to the left by 3 taking in to consideration the fact that there are 26 letters in the English alphabet. In order to return to the original letters one can simply shift each letter in the encrypted message to the right 3 more times. Therefore, the decryption key is 3. In most situations, the receiver needs to know only the decryption key.

Private key encryption involves the use of one key. This key is both the encryption and decryption key. Hence, the sender and receiver both need knowledge of the same key. Private key encryption is a relatively simple process as only one key is required for both encryption and decryption (Hoffstein, Pipher, & Silverman, 2008). In a perfect world, private key cryptography is sufficient to protect important information. However, most senders must worry about possible interference of their message. If the secret key landed in the hands of an adversary, then he or she could steal or alter confidential information with little effort. Even though private key encryption is simple in theory, in actuality it brings many security threats that make the method not secure.

Public key encryption, a much safer alternative to private key encryption, incorporates the use of two keys: one public key and one private key. The public key functions as the encryption key which means that any individual can use the public key to

encrypt a message, but only the owner of the private key, or the decryption key, can decrypt the encoded messages (Wang, Xu, & Wang, 2016). Although public key cryptography is more secure than private key cryptography, the method still involves several weaknesses, so the process of storing the secret key must be secure.

As in the case of public key cryptography, if an adversary discovers the private key, then he or she can also decrypt any encoded messages. As a result, many seek to improve the means in which they exchange the secret key using prime numbers, elliptic curves, and other more complex methods (Katz & Lindell, 2015). Another issue with public key cryptography involves the public key, itself. The public key does not need to be a secret key and will be published publicly. A third party, however, can intercept the releasing of the public key and alter it. This third party can also create a unique private key and decrypt any messages. In order to not raise any suspicions, the messages must also continually be intercepted, decrypted, and then encrypted once again using the fake public key.

Although this interception process certainly is possible, the more difficult the encryption/decryption process, the harder for an adversary to pull off such a trick. Some common examples of public key cryptography are the Diffie-Hellman key exchange and the ElGamal key generator. Both encryption systems involve the use of prime numbers and use the difficulty of factoring large primes to ensure more security (Katz & Lindell, 2015). Both processes will be discussed in detail later; however, one must first understand some fundamental mathematical concepts.

**Finite Fields**

Let $S$ be a set and $S \times S$ be the set of ordered pairs $(s, t)$ such that $s, t$ are elements of $S$. A *binary operation*, $*$ , maps $S \times S \rightarrow S$. Note that the image of $(s, t)$ in $S \times S$ must also be an element in $S$. A *group* is a set $G$ such that the following properties hold:

1. Associativity: For any $a, b, c \in G$, $a * (b * c) = (a * b) * c$.
2. Identity: For any $a \in G$, there exists an element $e$ such that $a * e = e * a = a$
3. Inverse: For any $a \in G$, there exists an inverse element $a^{-1}$ such that $a + a^{-1} = a^{-1} + a = e$.

The group is called an *abelian group* if the following property also holds:

4. Commutativity: For any $a, b \in G$ , $a * b = b * a$.

A *ring* is a set $R$ with two binary operations + and · that satisfy the following:

1. $R$ is an abelian group with respect to +.
2. The binary operation · is associative.
3. The distributive property holds. Hence, for any $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

A ring is called a *field* if in addition the following also hold:

4. The binary operation · is commutative.
5. The non-zero elements of $R$ form a group under · .

A *finite field* is simply a field that contains finitely many elements. The finite field $\mathbb{F}_p$ is the finite field containing all the elements mod $p$ (Mullen & Panario, 2013; Cohen, Frey, Avanzi, 2006).

## Key Exchanges over Finite Fields

The finite field $\mathbb{F}_p$ provides many important applications to the realm of cryptography. Perhaps one of the most relevant is the discrete logarithm problem. Note that a *primitive root* is an element $g$ in $\mathbb{F}_p$where the powers of $g$ generate the entire group of $\mathbb{F}_p$. The discrete logarithm problem is the difficulty of finding some $x \epsilon \mathbb{F}_p$ such that $g^x = h\ (mod\ p)$, where $g$ is a primitive root and h is any non-zero integer in $\mathbb{F}_p$. The discrete logarithm can be written as $x = \log_g h$. Note that $h = g \cdot g \cdot ... \cdot g\ (mod\ p)$ for $x$ multiplications of $g$. Essentially, in order to find $\log_g h$ one must find how many times g must be multiplied by itself in order to get $h$ (Hoffstein, Pipher, & Silverman, 2008).

An obvious way to compute the discrete logarithm is by testing out powers of $g$ one by one until some power $i$ such that $g^i = h\ (mod\ p)$. For example, to find an $a$ such that $2^x = 7(mod\ 11)$, test the powers of $2, 2^0, 2^1, \ldots 2^7$, and eventually find that $2^7 = 7\ (mod\ 11)$. However, this method becomes extremely difficult for any large prime number. Both the Diffie-Hellman key exchange and the ElGamal key generator base their computations on the difficulties surrounding the discrete logarithm (Katz & Lindell, 2015).

**The Diffie-Hellman Key Exchange**

Suppose two people, Alice and Bob, want to share a secret key, but Eve, an outside adversary, can intercept any exchange between the two. By using the difficulty of the discrete log problem to their advantage and the steps of the Diffie-Hellman key exchange, Alice and Bob can avoid Eve's obtaining of their key.

Alice and Bob must first agree on some large prime $p$ and a nonzero integer, $g$ in $\mathbb{F}_p$ which is available to the public, even to Eve. However, Alice also secretly chooses an integer $a$ which she uses to calculate $A = g^a (mod\ p)$. Meanwhile, Bob also chooses a secret integer $b$ and calculates $B = g^b (mod\ p)$. Alice then sends $A$ to Bob, while Bob sends $B$ to Alice. Alice takes $B$ and computes $B^a$, and Bob takes A and computes $A^b$. Since $B^a = A^b = g^{ab} (mod\ p)$, both Alice and Bob receive the key, $g^{ab} (mod\ p)$ without Eve also receiving the key (Katz & Lindell, 2015).

For example, assume Alice and Bob pick the prime number $p = 167$ and $g = 2$. So, Alice takes $p$ and $g$ and computes $A$, using her secret number $a = 23$ which only she knows. Bob also takes $p$ and $g$ and computes $B$, using his secret number $b = 55$ which only Bob knows. So, $A = 2^{23} \equiv 31 (mod\ 167)$ and $B = 2^{55} \equiv 50 (mod\ 167)$. Alice then sends Bob $A = 31$ and Bob sends Alice $B = 50$. With this new information, Alice computes $B^a$ and Bob computes $A^b$ such that $B^a = 50^{21} \equiv 150\ (mod\ 167)$ and $A^b = 31^{55} \equiv 150\ (mod\ 167)$. Hence, both Alice and Bob obtain the key, $k = 150$, without anyone else also receiving the key. Note that an adversary, Eve, can obtain the values of $A$ and $B$, but neither Eve nor Bob knows the value of $a$, and neither Eve nor Alice knows the value of $b$. This mean Eve would have to solve $2^a \equiv 31\ (mod\ 167)$ and $2^b \equiv 50\ (mod\ 167)$ in order to find the values of $a$ and $b$, which becomes extremely difficult, especially in a real life situation where the numbers are significantly larger.

**The ElGamal Key Generator**

ElGamal public key encryption closely resembles the Diffie-Hellman public key exchange and also involves the discrete logarithm problem. The differences between the

Diffie-Hellman and the ElGamal approach stem mostly from the calculation involved with producing the shared key.

Say Alice chooses a prime number $p$ and a primitive root modulo $p$, $g$. She then computes her public key by raising $g$ to her private key, $a$. So, $A = g^a (mod\ p)$. Alice then publishes this information so that anyone can encrypt a message using her public key, but only Alice can decrypt the message using her private key. If Bob wants to send a message $m$ to Alice, he must choose a random key $k$, which is called the *ephemeral key*, and compute $B_1 = g^k (mod\ p)$ and $B_2 = m \cdot A^k = m \cdot g^{ak} (mod\ p)$. Bob sends Alice both $B_1$ and $B_2$as a pair $(B_1, B_2)$ (Hoffstein, Pipher, & Silverman, 2008).

In order for Alice to decrypt the message, she must use her private key, $a$. Alice begins by calculating $x = B_1^a = g^{ak} (mod\ p)$. Then, she finds $x^{-1} = b\ (mod\ p)$ and computes $B_2 \cdot x^{-1} = m \cdot x \cdot x^{-1} = m$. Hence, Alice decrypts the encrypted message to obtain the original message $m$ (Hoffstein. Pipher, & Silverman, 2008).

As an example, let Alice choose $p = 179$ and $g = 2$. She then chooses her private key, $a = 63$ and computes $A = 2^{63} \equiv 63 (mod\ 179)$. She then releases $p$, $g$, and $A$ to the public. Now, suppose Bob wants to send Alice a message $m = 123$, so he picks a random integer $k = 131$ and computes $B_1 = 2^{131} \equiv 35 (mod\ 179)$ and $B_2 = 123 \cdot 62^{131} = 74 (mod\ 179)$. Bob then sends Alice the pair (35,74). Once Alice receives the pair, she calculates $x = 35^{63} \equiv 69 (mod\ 179)$ and $x^{-1} = 96 (mod\ 179)$. By using $B_2$ Alice can decrypt the encrypted message to find the original message $m$. Alice computes $B_2 \cdot x^{-1} = 74 \cdot 96 \equiv 123 (mod\ 179)$. Hence, Alice successfully decrypts the message, $m = 123$, sent to her by Bob.

Consider the issues with public key cryptography discussed earlier. Both the Diffie-Hellman key exchange and the ElGamal key generator help combat these issues; however, the issues do not disappear completely. In the case of the Diffie-Hellman key exchange, if Eve wants to obtain the private key shared by Alice and Bob, she needs both Alice's secret integer $a$ and Bob's secret integer $b$. Notice the difficulty in Eve obtaining both $a$ and $b$ since neither Alice nor Bob know both $a$ and $b$ (Katz & Lindell, 2015). Also, in the example for Diffie-Hellman, the prime number chosen is 167, but in real life examples, the prime number chosen are extremely large making the computations for Eve even more difficult. Nonetheless, large primes also make the computations difficult for Alice and Bob as well.

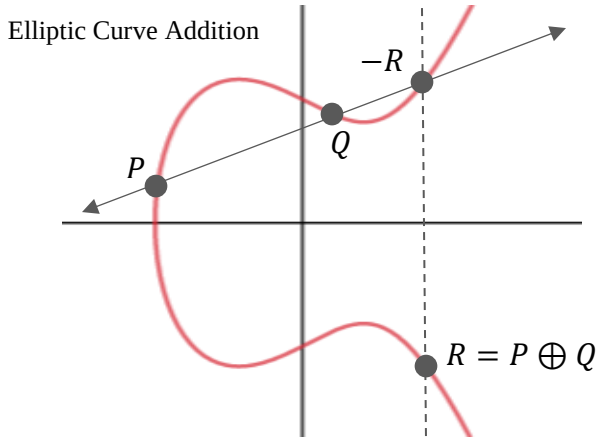
Regarding the ElGamal key generator, for Eve to decipher a message *m*, she not only deals with the repercussions of the discrete logarithm problem but also with the difficulty of modular inverses. Alice may still have a difficult time computing the modular inverse of $x$ even though she also has her secret key, $a$. Eve, without both Alice and Bob's secret keys, faces the daunting task of finding the correct exponent of $g$ in addition to then calculating the modular inverse of an exceedingly large number (Hoffstein. Pipher, & Silverman, 2008). Notice also that the message $m$ is a numerical value, so for longer messages the difficulty of the computations increases.

## Elliptic Curves

The use of elliptic curves in cryptography greatly improved the security of encryption ciphers, but what exactly is an elliptic curve? An *elliptic curve* over $\mathbb{F}_p$ is the set of solutions to an equation of the form $x^3 + ax + b$ where $a, b$ are elements of $\mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$. The form $x^3 + ax + b$ of an elliptic curve is known as the Weierstrass

form named after the German mathematician who discovered the form, Karl Weierstrass. The condition $4a^3 + 27b^2 \neq 0$ is also known as the discriminant of an elliptic curve (Silverman, 2009).

An important attribute of elliptic curves is addition over the curve. The binary operation $\oplus$ is called *elliptic curve addition*. Graphically, given two points $P$ and $Q$ on an elliptic curve $E$, we obtain $P \oplus Q$ by connecting a line $L$ from $P$ to $Q$ and finding the third intersection point labeled as $R$. By reflecting $R$ across the $x$-axis, one obtains $-R$ for which $P \oplus Q = -R$. Also, call $O$ the point at infinity, the identity for $E$, and say it exists at every vertical line (Hoffstein, Pipher, & Silverman, 2008).




Given an elliptic curve $E$ over $\mathbb{F}_p$ the following properties are also true:

1. Identity: $P \oplus O = O \oplus P = P$ for all $P$ in $E(\mathbb{F}_p)$.
2. Inverse: $P \oplus (-P) = O$ for all $P$ in $E(\mathbb{F}_p)$.
3. Associativity: $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$ for all $P, Q, R$ in $E(\mathbb{F}_p)$.
4. Commutativity: $P \oplus Q = Q \oplus P$ for all $P, Q$ in $E(\mathbb{F}_p)$.

Based on the previous definition of an abelian group, one can see that $E$ is an abelian group under elliptic curve addition. However, computing $\oplus$ graphically becomes

difficult and impractical when dealing with many additions. Thus, one can also use an elliptic curve addition algorithm (Hoffstein, Pipher, & Silverman, 2008).

Given an elliptic curve $E: y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ and two points $P_1, P_2 \in E(\mathbb{F}_p)$,

1. If $P_1 = O$, then $P_1 \oplus P_2 = P_2$.
2. If $P_2 = O$, then $P_1 \oplus P_2 = P_1$.
3. Else, let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$.
4. If $x_1 = x_2$and $y_1 = -y_2$, then $P_1 \oplus P_2 = O$.
5. Else, define λ as

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \; if \; P_1 \neq P_2 \\ \frac{3x_{1+a}^2}{2y\_1} \; if \; P_1 = P_2 \end{cases}$$

where $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$. Thus, $P_1 \oplus P_2 = (x_3, y_3)$. For example: Let $E(\mathbb{F}_{23})$: $y^2 = x^3 + x + 1$, $P_1 = (1,16)$, and $P_2 = (11,20)$. Since $P_1 \neq P_2$, $\lambda = \frac{20-16 \equiv 4}{11-1 \equiv 10} = 4 \cdot 10^{-1} = 4 \cdot 7 \equiv 5 (mod\ 23)$. Then use λ to compute $x_3$ and $y_3$ where $x_3 = 5^2 - 1 - 11 = 13 (mod\ 23)$ and $y_3 = 5(1 - 13) - 16 = 16 (mod\ 23)$. Thus, $P_1 \oplus P_2 = (13,16)$.

Recall that a Weierstrass equation of an elliptic curve is an equation of the form $y^2 = x^3 + ax + b$. However, this form is not defined for $\mathbb{F}_2$ or $\mathbb{F}_3$, so one must also consider a more general form of the Weierstrass equation suitable for all $\mathbb{F}_p$. The long Weierstrass form of an elliptic curve over $\mathbb{F}_p$ is

$E: y^2 + a_1xy + a_2 = x^3 + a_3^2 + a_4x + a_5$ where $a_1, a_2, a_3, a_4, a_5 \in \mathbb{F}_p$.

The long Weiestrass form works over any $\mathbb{F}_p$. Although, for the purposes of cryptography, the short Weierstrass equation is sufficient (Blake, Seroussi, & Smart, 2005). In fact, there exists an *isogeny* between the long Weierstrass form and the short Weierstrass form, meaning that the short Weierstrass from preserves the structure of an long form of an elliptic curve and can be used for cryptography. Given *E* and *E'* as two elliptic curves over $\mathbb{F}_p$, $\phi: E \to E'$ is an isogeny if 1) $x = u^2x' + r$ and 2) $y = u^3y' + u^2sx' + t$ where $(x, y) \in E, (x', y') \in E'$, and $u, s, t, r \in \mathbb{F}_p$ (Silverman, 2009).

Now, the fact that an elliptic curve with short Weierstrass form and an elliptic curve with long Weierstrass form an isogeny can be proven in the following manner:

*Proof.* Let *E'* be an elliptic curve with long Weiestrass form and *E* be an elliptic curve with short Weierstrass form over $\mathbb{F}_p$ such that,

$$E': (y')^2 + a_1x'y' + a_2{}' = (x')^3 + (a_3')^2 + a_4x' + a_5 \text{ and}$$

$$E: y^2 = x^3 + c_1x + c_2.$$

Beginning with *E'*, the first goal is to manipulate *E'* in such a way that *y* can replace $u^3y' + u^2sx' + t$ for some $u, s, t \in \mathbb{F}_p$.

$$(y')^2 + a_1x'y' + a_2y' = (x')^3 + (a_3x')^2 + a_4x' + a_5$$

$$(y')^2 + (a_1x' + a_2)y' + \frac{(a_1x+a_2)^2}{4} = (x')^3 + (a_3x')^2 + a_4x' + a_5 \ + \frac{(a_1x+a_2)^2}{4}$$

$$\left(y' + \frac{a_1x'+a_2}{2}\right)^2 = (x')^3 + \left(a_3 + \frac{a_1^2}{4}\right)(x')^2 + \left(a_4 + \frac{2a_1a_2}{4}\right)x' + (\frac{a_2^2}{4} + a_5)$$

By setting $y \ = \ y' + \frac{a_1}{2}x' + \frac{a_3}{2}$, the equation becomes

$$y^2 = (x')^3 + \left(\frac{4a_3+a_1^2}{4}\right)(x')^2 + \left(\frac{2a_4+a_1a_2}{2}\right)x' + \frac{4a_5+a_2^2}{4}.$$

In order to simplify the equation for future calculations, set $4a_3 + a_1^2 = b_1$, $2a_4 + a_1a_2 = b_2$, and $4a_5 + a_2^2 = b_3$. Thus, the equation is

$$y^2 = (x')^3 + \frac{b_1}{4}(x')^2 + \frac{b_2}{2}x' + \frac{b_3}{4}.$$

The next objective of the proof is to manipulate the equations further so that *x* can replace $u^2x' + r$ for some $u, r \in \mathbb{F}_p$.

$$y^2 = \left((x')^3 + \frac{b_1}{4}(x')^2 + \frac{b_1}{48}x' + \frac{b_1}{1728}\right) + \frac{b_2}{2}x' + \frac{b_3}{4} - \frac{b_1}{48}x' - \frac{b_1}{1728}$$

$$y^2 = \left(x' + \frac{b_1}{12}\right)^3 - \left(\frac{b_1^2}{48}x' - \frac{b_2}{2}x' + \frac{b_1^3}{576} - \frac{b_1b_2}{24}\right) - \frac{b_1^3}{1728} + \frac{b_3}{4} + \frac{b_1^3}{576} - \frac{b_1b_2}{24}$$

$$y^2 = \left(x' + \frac{b_1}{12}\right)^3 - \left(\frac{b_1^2 - 24b_2}{48}\right)\left(x' + \frac{b_1}{12}\right) - \frac{b_1^3 + 3b_1^3 + 432b_3 - 72b_1b_2}{1728}$$

$$y^2 = \left(x' + \frac{b_1}{12}\right)^3 - \left(\frac{b_1^2 - 24b_2}{48}\right)\left(x' + \frac{b_1}{12}\right) - \frac{b_1^3 - 36b_1b_2 + 216b_3}{864}$$

By letting $x = x' + \frac{b_1}{12}$,

$$y^2 = x^3 - \frac{b_1^2 - 24b_2}{48}x - \frac{b_1^3 - 36b_1b_2 + 216b_3}{864}.$$

Notice for $c_1 = \frac{24b_2 - b_1^2}{48}$ and $c_2 = \frac{b_1^3 - 36b_1b_2 + 216b_3}{864}$,

$$y^2 = x^3 + c_1x + c_2 = E.$$

The substitutions $y = y' + \frac{a_1}{2}x' + \frac{a_3}{2}$ and $x = x' + \frac{b_1}{12}$ follow the definition of an isogeny where $u = 1, t = \frac{a_3}{2}, s = \frac{a_1}{2}$, and $r = \frac{b_1}{12}$. Thus, there exists an isogeny such that $\phi: E \to E'$ and $(x, y) \mapsto \left(x' + \frac{b_1}{12}, y' + \frac{a_1}{2}x' + \frac{a_3}{2}\right)$. Therefore, the structure of an elliptic curve is preserved when using the short Weierstrass form, and this form can be used for elliptic curve cryptography (Silverman, 2009).

An important attribute of elliptic curves is the fact that the curve is non-singular and smooth, which ensures that the curve contains unique solutions. Without the characteristic of being non-singular, elliptic curves could not be used for cryptography. Hence, the condition $4a^3 + 27b^2 \neq 0$, or the discriminant, assures that the curve is, in fact, non-singular (Cohen, Frey, & Avanzi, 2006). Essentially, the discriminant of an elliptic curve implies that there is a tangent line at every point, thus E is non-singular and smooth. One can prove that the discriminant is $4a^3 + 27b^2 \neq 0$ in the following manner:

*Proof.* Let $f(x, y) = y^2 - x^3 - ax - b$. Then, $\frac{\partial f}{\partial x} = -3x^2 - a$ and $\frac{\partial f}{\partial y} = 2y$.

Hence, $\frac{\partial y}{\partial x} = \frac{3x\text{^}2 + a}{2y}$, and notice that $\nabla f = \langle 3x^2 + a, 2y \rangle$. $E$ is smooth if $\nabla f$ exists and is nonzero at $\langle \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y} \rangle$. So, find where $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ are both equal to zero. When $\frac{\partial f}{\partial x} = 0, a = -3x^2$ and when $\frac{\partial f}{\partial y} = 0, y = 0$. Thus, when $a = -3x^2$ and $y = 0$,

$$f(x, 0) = -x^3 - (-3x^2)x - b = 2x^3 - b.$$

In order to ensure that $E$ is non-singular, set $f = 0$ and then restrict the result. Hence, $2x^3 - b = 0$ and thus $x^3 = \frac{b}{2}$. Notice that $a = 3x^2$, so $a^3 = -27x^6$ and $x^6 = -\frac{a^3}{27}$. Therefore,

$$\left(\frac{b}{2}\right)^2 = x^6 = -\frac{a^3}{27}.$$

So, $-27b^2 = 4a^3$ and thus $4a^3 + 27b^2 = 0$.

Remember that in order for $E$ to be non-singular, one must restrict the values $a$ and $b$ such that $4a^3 + 27b^2 \neq 0$. Therefore, since the restriction ensures that $\nabla f$ exists and is nonzero at every point of the curve, the discriminant of an elliptic curve implies that there

is a tangent line at every point; thus, $E$ is non-singular and smooth. Now, one can properly understand the cryptographic applications of elliptic curves.

A similar discrete logarithm problem occurs with elliptic curves. However, the discrete logarithm problem for elliptic curves involves elliptic curve addition instead of multiplication. Thus, the elliptic curve discrete logarithm problem is the problem of finding some $n$ such that $Q = P \oplus P \oplus \ldots \oplus P$ where $P$ is added to itself $n$ times (Cohen, Frey, & Avanzi, 2006). Formally, Given an elliptic curve over $\mathbb{F}_p$ and points $P$, $Q$ in $\mathbb{F}_p$, the *elliptic curve discrete logarithm* problem is the problem of finding an $n$ such that $Q = nP$, where one writes $n = \log_P Q$. Next, consider how the elliptic curve discrete logarithm problem changes the approach to the Diffie-Hellman key exchange and the ElGamal key generator.

**Diffie-Hellman Elliptic Curve Key Exchange**

Elliptic curves can also be used to exchange keys using the Diffie-Hellman key exchange. However, instead of choosing a prime number $p$ and a nonzero integer $g$ in $\mathbb{F}_p$, Alice and Bob must choose $p$, an elliptic curve over a finite field $E(\mathbb{F}_p)$, and a point $P$ in $E(\mathbb{F}_p)$ (Cohen, Frey, & Avanzi, 2006). Note that the Diffie-Hellman key exchange with elliptic curves uses elliptic curve addition, not multiplication as in the key exchange for $\mathbb{F}_p$.

After Alice and Bob agree on $E(\mathbb{F}_p)$ and $P$, Alice picks a secret integer $a$ and she computes $Q_a = aP$. Meanwhile, Bob picks a secret integer $b$ and computes $Q_b = bP$. Alice then sends $Q_a$ to Bob, and Bob sends $Q_b$ to Alice. Both Alice and Bob use their

respective secret integers $a$ and $b$ to compute $aQ_b = abP = bQ_a$, which becomes a secret key shared by Alice and Bob (Cohen, Frey, & Avanzi, 2006).

Specifically, say Alice and Bob agree on $E(\mathbb{F}_{3023})$: $y^2 = x^3 + x + 2547$ and $P = (2237,2480)$ where $P \epsilon E(\mathbb{F}_{3023})$. Alice then chooses a secret integer $a = 2313$ and calculates $Q_a = 2313P = (934, 29)$. Meanwhile, Bob also chooses a secret integer $b = 1236$ and calculates $Q_b = 1236P = (1713,1709)$. Then, Alice sends $Q_a$ to Bob, and Bob sends $Q_b$ to Alice. By using their respective secret integers, $a = 2313$ and $b = 1236$, both Alice and Bob obtain the secret key $2313Q_b = 1236Q_a = (2537,1632)$.

Even though both the Diffie-Hellman key exchange over $\mathbb{F}_p$ and $E(\mathbb{F}_p)$ involve similar processes, the recommended key size for the elliptic Diffie-Hellman key exchange is significantly smaller than that for the key exchange over $\mathbb{F}_p$. According to NIST, a 3072-bit key or larger is recommended for the Diffie-Hellman key exchange over $\mathbb{F}_p$, while only a 384-bit is recommended for the elliptic Diffie-Hellman key exchange (Barker, 2016). Thus, the Diffie-Hellman elliptic curve key exchange can provide sufficient security with a significantly smaller key than the Diffie-Hellman key exchange over finite fields.

**The ElGamal Elliptic Curve Key Generator**

Elliptic curves also provide application to ElGamal cryptosystems. Alice chooses a prime number $p$, an elliptic curve $E(\mathbb{F}_p)$, and a point $P$ in $E(\mathbb{F}_p)$. After she chooses a secret key $a$, she then computes $Q_a = aP$ and publishes $Q_a$, along with $p$, $E(\mathbb{F}_p)$, and $P$. Now, if Bob wants to send a message $M$ in $E(\mathbb{F}_p)$ to Alice, he chooses a random integer

$k$ to be his ephemeral key and then computes $B_1 = kP$ and $B_2 = M \oplus kQ_a$. Bob sends $(B_1, B_2)$ to Alice. Alice then takes the pair from Bob and using her secret key a computes

$$B_2 - aB_1 = (M \oplus kQ_a) - akP = M \oplus akP \oplus -akP = M.$$

Thus, Alice receives the original message $M$ (Hoffstein, Pipher, & Silverman, 2008).

Now, suppose Alice chose $p = 3023$, $E(\mathbb{F}_{3023})$: $y^2 = x\text{^}3 + x + 2547$, and $P = (2237,2430)$. Alice chooses a secret key $a = 2313$, and computes $Q_a = 2313P = (934,29)$ which Alice makes available to the public along with $p$,$E(\mathbb{F}_{3023})$, and $P$. Bob decides that he wants to send Alice a message $M = (2181,4000)$ in $E(\mathbb{F}_{3023})$, so he chooses a random integer $k = 1236$ and calculates $B_1 = 1236p = (1713,1709)$ and $B_2 = (2181,400) \oplus 1236Q_a = (2181,400) \oplus (2537,1632) = (2720, 452)$. Bob sends Alice $(B_1, B_2)$ where $B_1 = (1713, 1709)$ and $B_2 = (2720, 452)$. Alice receives $(B_1, B_2)$ and uses her secret key a to obtain the original message $M$.

$B_2 - aB_1 = (2720, 452) \oplus -2313B_1 = (2720, 452) \oplus (2537, -16) = (2181, 400)$

Since $(2181, 400) = M$, Alice obtains the original message.

**Advantages and Disadvantages of Elliptic Curve Cryptography**

After looking at the application of elliptic curves to the Diffie-Hellman key exchange and the ElGamal key exchange, the efficiency of elliptic curves in securing private information is apparent. Elliptic curves add a unique layer to cryptography and elliptic curve addition provides a way to apply methods in $\mathbb{F}_p$ to $E(\mathbb{F}_p)$ instead (Xiong, Qin, & Vasilakos, 2017). Though the general public may be unaware of elliptic curves and their applications, their importance to cryptography is apparent just with their addition to public key exchanges.

However, even elliptic curve cryptography faces several disadvantages. First of all, the computations with elliptic curve cryptography involve more complex mathematics. While the computations surrounding public key cryptography over finite fields make sense even without a full understanding of the mathematics behind the system, understanding the process of elliptic curve cryptography and the addition process comes less from common knowledge and more from extensive research (Silverman, 2009). Elliptic curve addition adds multiple steps to the encryption and decryption process, so the likelihood of implementation errors increases. Also, elliptic curve addition significantly increases the key size compared to basic multiplication making the computations even more difficult.

## Quantum Mechanics

Even with the mathematical advancements thus far, security breaches still exist as none of the cryptographical methods are unbreakable. However, the quantum realm offers a unique perspective on cryptography and multiple other areas of study (Sergienko, 2006). Before diving into the complexities of quantum cryptography, one should seek understanding of the laws associated with the quantum realm.

Quantum mechanics describes the actions of atoms and subatomic particles. When looking at the nature of the quantum realm, one must understand that particles act according to a completely different set of rules than the visible world (Griffiths, 2006). Consider a car driving down a road; one can easily find the position of the car at a certain time, as well as the velocity and mass by taking basic measurements. Quantum particles, however, do not act according to classic physics.

German physicist, Werner Heisenberg, studied the nature of particles and discovered a key component of quantum particles: the momentum and position of a particle cannot be known with full certainty. The uncertainty principle states that the inaccuracy of the position of a particle multiplied by the inaccuracy of the momentum of a particle must be larger than $\frac{h}{4\pi}$, where $h$ is Planck's constant (Griffiths, 2006). Essentially, the uncertainty principle says the more one knows about the position of a particle, the less he or she knows about the momentum and vice versa. Even the very act measuring a quantum system disturbs the system, itself. Thus, one cannot know the precision of the position and momentum of a particle with absolute certainty. Mathematically, the uncertainty principle says $\Delta x \Delta p > \frac{h}{4\pi}$ where $x$ is the position and $p$ is the momentum of a particle (Griffiths, 2006).

Think of electrons circling a nucleus. Knowing that opposite charges attract, one might think that the electrons would be attracted all the way to the positively charged nucleus. However, the certainty of the electrons' location close to the nucleus implies that the uncertainty of the electrons' momentum would be enormous. Thus, the electrons may be moving so fast that they leave the atom entirely (Griffiths, 2006; Horodecki, 2010). Remember the example of the car driving down a road. The observability of the position and momentum of the car makes it hard to believe that the particles which make up the car are acting in a manner contrary to the observable car.

Particles at the subatomic level move similar to waves. An important property of waves is that waves can be added together to produce another wave. This property can also be applied to quantum states. Two quantum states can be added together to produce

another quantum state. This idea that particles can be in two states at the same time id called superposition. One practical example of superposition in motion is the qubit. A classical bit, or binary digit, can only appear as one of two states, usually either 1 or 0. In contrast, qubits can also appear as the superposition of 1 and 0 thereby existing as two states at the same time (Sergienko, 2006).

An interesting aspect of the quantum realm is the phenomenon known as entanglement. Entanglement occurs when the quantum state of a pair or group of particles exist dependently upon one another (Griffiths, 2006). Entangled particles essentially cannot be described without each other, and a correlation exists between the particles even over a physical distance.

To understand the idea of entangled particles, picture a pair of gloves, one right-handed glove and one left-handed glove. Now, suppose that an individual places each glove in a box and ships them to two different locations where Person 1 waits at one location and Person 2 waits at the other location. Once both individuals receive their boxes, Person 1 opens his boxes to reveal a left-handed glove, so Person 2's box must contain a right-handed glove. Notice that the moment that Person 1 opened his box and a left-handed glove was revealed, Person 2 could only have a right-handed glove. Entangled particles act in the same manner, once a certain physical attribute of one particle is revealed, the other particle(s) act in accordance (Griffiths, 2006; Horodecki, 2010). The idea of entanglement and superposition plays a crucial role in quantum cryptography.

## Quantum Cryptography

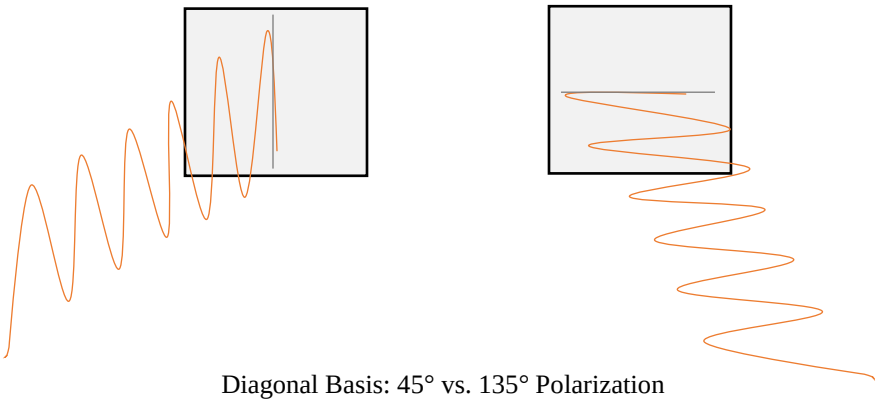
Several features of quantum mechanics provide useful applications to cryptography. A well-known application of quantum mechanics to cryptography is with quantum key distributions. The ability to send information through quantum particles eliminates many of the issues with the usual key distribution methods (Horodecki, 2010). Remember the very act of measuring particles disturbs the systems leading to even more uncertainty about the position or momentum of a particle. Hence, the moment that an adversary attempts to eavesdrop or intercept the key exchange between two parties, they can immediately detect a disturbance.

Most quantum key distributions use the polarization of photons in order to exchange information. Light emitting diodes, or LEDs, enable an individual to control the creation of the photons by making one single photon at a time. Also, a polarization filter allows for only photons with a certain polarization to pass through the filter while blocking all other photons from coming through (Sergienko, 2006). The difficulty with measuring polarization is that once the photons are polarized, they cannot be measured again without disrupting the polarization of the photons, itself, in the process. Quantum key exchanges rely on attaching information to a photon and knowing the original polarization of the photon (Sergienko, 2006). How can one know the original polarization of the photon when the very act of measuring the polarization disturbs the polarization itself?

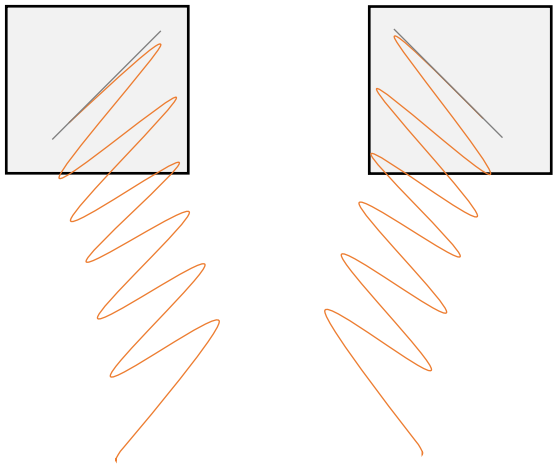
First, one must determine which types of polarizations to use. The two most well-known polarization bases are rectilinear and diagonal polarization, and it is important to note that a polarization base must consist of two orthogonal states. The rectilinear basis includes a vertical polarization of 0°, meaning the photons move in an up and down

oscillating motion, and a horizontal polarization of 90°, meaning the photons move in a side to side oscillating motion. The diagonal basis uses a polarization of 45° and 135°. Notice that these angles are also orthogonal, so a polarization of 45° correlates to a wave-like motion at 45°, and a polarization of 135° correlates to a wake-like motion at 135° (Sergienko, 2006).

Rectilinear Basis: Vertical vs. Horizontal Polarization

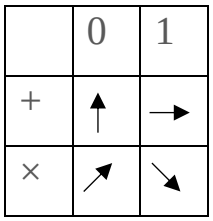


Diagonal Basis: 45° vs. 135° Polarization



The first quantum cryptography protocol, known as BB84, uses two orthogonal states, usually the rectilinear basis and the diagonal basis. The protocol then assigns a 0 bit to both 0° and 45° and a 1 bit to both 90° and 135° (Sergienko, 2006). Also, the rectilinear basis is labeled by the symbol + and the diagonal basis is labeled by the

symbol ×.




To better understand the steps of the quantum key exchange, suppose Alice and Bob want to share a message through some quantum communication channel, likely an optical fibre or a vacuum, and any adversary, Eve, can try any approach to mess up the communication within the quantum channel. Also, Alice decides to use the rectilinear basis and the diagonal basis as her orthogonal bases. She starts by randomly choosing a 0 or 1 bit and then randomly choosing a basis as well. Say Alice randomly chooses a 1 bit and the diagonal basis. She then transmits a photon to Bob in the horizontal state according to the diagonal basis at 135° (Horodecki, 2010).

Bob receives the photon and randomly chooses either a rectilinear or diagonal filter to measure the photon assuming that Bob is unaware of what basis Alice used to polarize the photons. When Bob finishes measuring the photons sent by Alice, he communicates to Alice. Alice and Bob then discuss over the channel where Bob says the basis he used to measure each photon and Alice says whether Bob is correct or incorrect in lining up with how she polarized the photons. They both discard the bits where Bob used a different basis and thus, the key is the remaining bits (Horodecki, 2010).

Specifically, say Alice and Bob decide to use the quantum key exchange with the rectilinear and diagonal bases. Alice sends eight photons randomly using the method

described above, and Bob measures the photons he receives randomly. They receive the following information after discussing through a quantum communication channel.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Alice's Bit | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| Alice's Random Basis | + | × | × | + | + | + | × | + |
| Alice's Angle | 0° | 45° | 135° | 0° | 90° | 90° | 135° | 0° |
| Bob's Random Measurement | + | + | × | × | + | × | + | + |
| Bob's Angle | 0° | 90° | 135° | 45° | 90° | 135° | 90° | 0° |
| Matches | X | | X | | X | | | X |
| Shared Key | 0 | | 1 | | 1 | | | 0 |

So, Alice and Bob both receive the shared secret key 0110. Also, notice that for the photon polarizations where the basis does not line up, the photon detector randomly chooses between vertical and horizontal polarization (Sergienko, 2006).

## Conclusion

After looking through the different techniques of cryptography, one clearly sees how mathematics has impacted the realm of cryptography. However, as mathematics evolves and the level of security grows with each newly implemented cryptographical method, adversaries also grow in knowledge and understanding of the underlying process of security. Thus, just as mathematics is always evolving, the application of mathematics to cyber security must also be growing. Each cryptographical method discussed, contains advantages and disadvantages concerning its respective encoding and decoding processes. Public key cryptography of a finite field proves the simplest to calculate and understand but requires a larger key size in order to reach the level of security of elliptic curve cryptography. Although elliptic curve cryptography allows for a smaller key size, the complex mathematical techniques leave room for calculation errors and confusion.

Quantum cryptography seems to excel in many areas where the other methods fail. However, the distance over which quantum cryptography can take place is still lacking. Considering that researchers have only just scratched the surface of the quantum realm, as time goes on and knowledge progresses, cryptographical techniques will continue to advance.

References

Barker, E.(2016). Recommendation for key management part 1. *NIST Special Publication*. doi:10.6028/nist.sp.800-57pt1r4

Blake, I. F., Seroussi, G., & Smart, N. P. (2005). *Advances in elliptic curve cryptography*. New York: Cambridge University Press.

Budiansky, S. (2016). *Code warriors: NSA's codebreakers and the secret intelligence war against the Soviet Union*. New York: Vintage Books.

Chen, N. (2017). China' s quantum satellite establishes photon entanglement over 1,200 km. Retrieved from http://english.cas.cn/newsroom/news/ 201706/t20170619_178279.shtml.

Cohen, H., Frey, G., & Avanzi, R. (2006;2005;). *Handbook of elliptic and hyperelliptic curve cryptography* (1st ed.). Boca Raton, FL: Chapman & Hall/CRC.

Dooley, J. F. (2018). *History of cryptography and cryptanalysis: codes, ciphers, and their algorithms*. Cham: Springer Nature.

Griffiths, D. (2006). *Introduction to quantum mechanics* (Second edition.). Upper Saddle River, NJ: Pearson Prentice Hall.

Hoffstein, J., Pipher, J., & Silverman, J. H. (2008). *Introduction to mathematical cryptography*. New York: Springer-Verlag New York.

Horodecki, R. (2010). *Quantum cryptography and computing: theory and implementation.* IOS Press.

Katz, J., & Lindell, Y. (2015). *Introduction to modern cryptography* (Second ed.). London: CRC.

Middleton, B. (2017). *A history of cyber security attacks: 1980 to present* (1st ed.). Philadelphia: CRC.

Mollin, R. A. (2003). *RSA and public-key cryptography* (1st ed.). Boca Raton, FL: Chapman & Hall/CRC.

Mullen, G., & Panario, D. (2013). *Handbook of finite fields*. Boca Raton, FL: CRC.

National Security Agency: central security service defending our nation. (2015). Retrieved from https://apps.nsa.gov/iaarchive/ programs /iad-binitiatives/cnsa-suite.cfm

Sergienko, A. V. (2006*). Quantum communications and cryptography* (1st ed.). Boca Raton, FL: Taylor & Francis.

Silverman, J. H. (2009). *The arithmetic of elliptic curves* (Second ed.). New York: Springer-Verlag.10.1007/978-0-387-09494-6.

Wang, X., Xu, G., Wang, M., & Meng, X. (2016). *Mathematical foundations of public key cryptography* (1st ed.). Boca Raton, FL: CRC.

Washington, L. C. (2003). *Elliptic curves: number theory and cryptography*. Boca Raton, FL: Chapman & Hall/CRC.

Xiong, H., Qin, Z., & Vasilakos, A. (2017). *Introduction to certificateless cryptography*. Boca Raton, FL: CRC/Taylor & Francis.

Yan, S. Y., & Springer Science+Business Media. (2008). *Cryptanalytic attacks on RSA*. New York: Springer.