A Comparison of Cryptographic Methods

C. Noah Gilmore

A Senior Thesis submitted in partial fulfillment
of the requirements for graduation
in the Honors Program
Liberty University
Fall 2022

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.

_____

Timothy Sprano, Ph.D.
Thesis Chair

_____

David Wang, Ph.D.
Committee Member

_____

James H. Nutter, D.A.
Honors Director

_____

Date

Abstract

While elliptic curve cryptography and quantum cryptography are significantly different branches of cryptography, they provide a suitable reference point for comparison of the value of developing methods used in the present and investing in methods to be used in the future. Elliptic curve cryptography is quite common today, as it is generally secure and efficient. However, as the field of cryptography advances, the value of quantum cryptography's inherent security from its basic properties should be considered, as a fully realized quantum cryptosystem has the potential to be quite powerful. Ultimately, it is of critical importance to determine the value of investing in strengthening current cryptosystems in comparison to seeking to accelerate the development of new ones. While both are of importance, the question should be asked if one avenue of development will be more effective overall.

A Comparison of Cryptographic Methods

Cryptography refers to the practice of encrypting, sending, and decrypting information in order to protect that information from any enemies that would wish to know and exploit it. It is commonly employed by any technological system that needs to keep some amount of information private, be it personal user data on the internet or government secrets that cannot fall into enemy hands. Regardless of why it may be employed, cryptography is an important practice for any entity in an increasingly digital age, where new methods to protect and attack information systems are constantly in development.

For this discussion of cryptography, an appropriate place to begin would be with a definition of terms. *Plaintext* is used to describe the information that needs to be encrypted, transmitted, and decrypted; it is the information that the two communicating parties wish to share privately. *Ciphertext* refers to how the information reads as it is sent. Ciphertext is a string of symbols or characters, usually numbers, representing the plaintext in some way, which needs to be deduced through the methods used for encryption and decryption, depending on the processes used. Plaintext is converted to ciphertext through use of a *key*. While some cryptographic systems employ multiple keys, every system uses at least one key that is kept private, known only to the two communicating parties. The task of the attacker is to acquire the ciphertext and the key without being detected by the two communicating parties, and decrypt the plaintext. When discussing the scenario of two parties seeking to exchange information, with an outside party seeking to intercept that information, this paper will conform to the standard practice of designating the party sending the information as *Alice*, the intended recipient as *Bob*, and the party attempting to eavesdrop as *Eve*.

In a standard cryptographic procedure, Alice seeks to send some amount of sensitive information to Bob. They have a channel through which to communicate, but the potential for Eve to access that channel also exists. Alice must therefore take her plaintext and convert it into ciphertext, based on the methods being used in that particular situation. The strategies employed will detail the particulars of the key, how the ciphertext is sent to Bob, and how he can receive the key he needs to decrypt the ciphertext. If Eve is unable to acquire both the ciphertext and the key, then the communication will have been successful. Many strategies will also have countermeasures present to make this more challenging for Eve than if she simply needed to break the base form of the cryptographic strategy.

Cryptography began with more simple methods, such as the scytale, a simple device comprised of a wooden cylinder and a strip of a material such as leather. Early ciphers did not employ much more than simple transposition of letters to hide the messages being sent. As the need for more sophisticated methods arose, new methods and systems have been developed throughout history to continue to protect important information from enemies (Bruss et al., 2007). Now the field has advanced to a point of integrating far more complex mathematical processes in order to keep up with humanity's advancements in mathematics and computation. As the abilities of outside parties to crack codes and algorithms grows more advanced, so too must the sophistication of the codes and algorithms employed increase.

As there are a variety of cryptographic methods currently in use, this thesis will use elliptic curve cryptography as a representative of present methods. While there are many others that could be used for this comparison, elliptic curve cryptography is one of the most widely used and is considered to be one of the more effective strategies currently employed. This will be

compared to quantum cryptography, a method that while still in development has already shown that it will be incredibly effective, as the transmission of data through particles such as photons makes it usually impossible for an interloper to even read the data being sent without alerting the two communicating parties.

As advancements are made in cryptography, the methods employed must be improved upon or replaced. Developments in quantum computing will eventually lead to more widespread use of quantum systems in cryptography, and will render older methods obsolete. However, the development of quantum cryptography is not yet at a point where such widespread use is feasible. As this is the case, there must be a discussion of the relationship between improvement of past methods and development of new ones. While both must certainly take place, it must be asked whether one is a priority. This question is the intention of this thesis.

This comparison is not being made in the sense of pitting two contemporaries against one another to determine a more effective strategies. Instead, this comparison appeals to the prioritization of general development. As time goes on, humans will always continue to experiment and learn in a variety of fields. As new information is discovered and learned, it is implemented as the relevant technology allows. When that development leads to new technologies, the cycle continues, and the potential for further complexity, in this case in the field of cryptography, continues to grow. However, research and development does require an allocation of resources, be they people, technological assets, or others. The purpose, then, of this comparison, is to determine whether, for any arbitrary scenario, with whatever resources may be available to the parties involved, priority should be given to the fortification of old strategies or the development of new ones. Both will inevitably occur, and both should; to utterly neglect

either option would be foolish, especially when dealing with cryptography, as it opens the door for extreme vulnerability in the near future or distant future, depending on the area of neglect. The question must be asked, however, whether it is worth it to risk being left behind, so to speak, in the area of quantum cryptography, or to risk an increased vulnerability in present-day strategies.

Elliptic Curve Cryptography

In order to discuss elliptic curve cryptography, an understanding of how elliptic curves function is necessary. To do so, definitions of abelian groups and finite fields is necessary, as elliptic curves are defined within those fields.

Abelian Groups and Finite Fields

Consider a set of numbers G. An abelian group involves a set of numbers, as well as some binary operation, meaning an operation that maps the set $G \times G$ into G. A symbol such as * can be used to represent the operation, although any symbol and corresponding operation may be used, so long as they are adequately defined. An abelian group is expressed as $(G, *)$, and all of its elements must conform to four conditions:

1. Associativity; for any elements $a, b, c \in G$, $a * (b * c) = (a * b) * c$.
2. Identity: there must exist an identity element in G. This element, referred to here as e, must satisfy the condition that $a * e = e * a = a$ for any element $a \in G$.
3. Inverses: every element $a \in G$ must have an inverse in G, notated here as a^{-1}, such that $a * a^{-1} = a^{-1} * a = e$, the identity element defined above.
4. Commutativity: for all elements $a, b \in G$, $a * b = b * a$.

The definition of a field stems from the definition of an abelian group: a field consists of a set of numbers, H, and two operations, usually described as addition and multiplication, notated $+$ and $*$ respectively (however, as previously, these principles can be applied to any two operations so long as they are sufficiently defined). There are three conditions for a field:

1. $(H, +)$ is an abelian group where 0 is the identity element. This is called the additive identity.
2. $(H, *)$ must be an abelian group with 1 as the identity element. This is called the multiplicative identity.
3. The distributive property holds: for any elements $f, g, h \in H$,

   $(f + g) * h = (f * h) + (g * h)$.

It should also be noted that if set H has a finite number of elements, then the field $(H, +, *)$ is a finite field (Dhanda et al., 2020).

Elliptic Curves

In general, an elliptic curve presents all the points in a finite field that satisfy the equation $y^2 = x^3 + ax + b$, where a and b are elements of that finite field. This curve also includes the point at infinity, which serves as the identity element for the additive abelian group formed by the points on the curve (Koblitz et al., 2000).

Elliptic Curves in Cryptography

Elliptic curve cryptography involves taking the elliptic curve defined over a finite field, generally chosen based on one of three models, and encrypting information through a method of mapping portions of the data to corresponding points on the curve. The first of these three models, the Weierstrass model, has already been introduced: curves are selected based on the

equation $y^2 = x^3 + ax + b$, which can be used to describe any elliptic curve defined over a large prime field. The other two models are as follows:

1. the Twisted Edwards Curve model, which uses the equation

   $ax^2 + y^2 = 1 + dx^2y^2$, where a and d are elements of the field

2. the Montgomery model, using the equation $By^2 = x^3 + Ax^2 + x$, where A and B are elements of the field.

(Dhanda et al., 2020)

This process is usually considered secure because of the discrete logarithm problem (DLP), which states: "given an elliptic curve E defined over F_q , a point $P \in E(F_q)$ of order *n*, and a point $Q \in E(F_q)$, determine the integer $l, 0 \leq l \leq n - 1$, such that $Q = lP$, provided that such an integer exists" (Koblitz et al., 2000, p. 179). In this definition, F_q is the finite field over which the elliptic curve is defined. This problem becomes more of a challenge for an enemy to decode when the party designing the key chooses a sufficiently large prime number for n. Additionally, as outlined by Scholl, the difficulty of the DLP can be further increased by selecting a *super-isolated* elliptic curve. A curve is super-isolated if its isogeny class contains only one isomorphism class. This results in curves that are more difficult to determine for an attacker than usual, since the majority of prime fields do not contain them (2019, p. 386). The difficulty of solving the discrete logarithm problem quickly and efficiently has generally resulted in secure transmissions through an elliptic curve system.

Elliptic Curve Cryptography is a public-key system, meaning that it employs two keys, one public and one private, for cryptographic practices. So long as the private key remains

private, the public key can be released on any channel, and it will be useless to any attacker lacking access to the private key (Bahramian & Hajirezai, 2020; Dhanda et al., 2020).

The Elliptic Curve Cryptography (ECC) Process

The standard ECC process as outlined by Dhanda et al. is comprised of three algorithms, each yielding an important piece of the process. The algorithms generate a key pair, carry out an encryption process, and a decryption process. In these algorithms, all references to "addition" and "multiplication" refer to the general operations; specifics will vary based on the field being used in a particular instance of the cryptography.

For the generation of a key pair, the generator of a cyclic subgroup within the finite field as well as an element of that subgroup are used to generate the public and private keys. The public key is created by using the field's "multiplication" operation on an element of the subgroup and the subgroup itself. This of course means the challenge for an adversary is determining which of the many subgroups and elements of those subgroups were used to determine the public key. The private key is the element of that cyclic subgroup that was used.

The encryption algorithm requires the selection of the elliptic curve upon which the data will be mapped. After converting the plaintext to points on the curve, the algorithm generates ordered pairs as the ciphertext. The first coordinate in the pair is the result of "multiplying" a different element of the same cyclic subgroup by that subgroup. The second coordinate results from "adding" the value on the curve that was originally mapped to and the "product" of the public key and the element of the cyclic subgroup used to determine the first coordinate.

The receiving party, Bob, must only carry out one step to decrypt the information received. By "adding" the additive inverse of the "product" of the private key and the first

coordinate to the second coordinate, he will be able to determine the initial value that was mapped along the curve. From this, the information needing to be sent can be extracted, thus resulting in a successful transmission (2020).

Applications and Additional Methods

Many methods of cryptography use elliptic curves as a component, while adding other computations, ultimately increasing the security of the information to be passed. Additionally, many uses for elliptic curve cryptography exist, both as ways to transmit information and as ways to use the transmission techniques to accomplish other goals, such as verifying a user.

User Authentication

Kumari et al. (2019) presented a method of using ECC to verify that two users communicating are in fact each other, rather than some other party. The system relies on a private key generator, independent of Alice of Bob, and allows them to each receive partial keys through an identification string. These partial keys require implementation into verification of other conditions determined by the particulars of the current session, and these are used to develop the full keys that Alice and Bob will use to communicate.

Scalar Multiplication

One method presented by Aljamaly and Ajeena (2021) uses elliptic scalar multiplication; that is, the data is encrypted based on a scalar multiplication graph, which involves the adjacent points of an elliptic curve being linked by scalar multiplication, resulting in a graph with weighted edges that matrices of encrypted data can be further encrypted along. By integrating matrices, the usual matrix benefits of carrying out operations on large quantities of data in less time can be employed in cryptography.

Isogenies of Elliptic Curves

Another method uses the fact that the set of points on an elliptic curve form an abelian additive group to develop a method based on isogenies. An isogeny maps one set of elliptic curve points to another, with the stipulation that the point at infinity for the first set maps to the point at infinity for the second set. By using a secure third party to construct public and private keys based on isogenies and identification strings, encrypted data can be transmitted securely based on standard elliptic curve measures as well as the difficulty of determining an isogeny based only on a single point mapping (Bahramian & Hajirezai, 2020).

Strengths

Elliptic curve cryptography is quite efficient, as the keys are usually smaller due to the nature of the encryption scheme (Dhanda et al., 2020). Other systems often have to carry out more calculations or choose larger primes as a starting point for encryption, but the complexity of the elliptic curve is such that similar security thresholds can be reached with less effort. Additionally, the aforementioned discrete logarithm problem makes it particularly challenging for any attacker to crack the system in a reasonable amount of time.

Weaknesses

Elliptic curve cryptography is not without its weaknesses. The main challenge for attackers of ECC is to solve the Discrete Logarithm problem efficiently. Ultimately, while there are strategies to crack an elliptic curve encryption, they still take time to execute, and a sufficiently complex elliptic curve system should be able to carry out its communication objectives before it could reasonably be broken by an attacker’s computing power.

A Shor's Algorithm Variant

One threat to the security of ECC is a variant of Shor's algorithm designed specifically to break elliptic curve systems. The more well-known Shor algorithm was developed in order to quickly find prime factorizations of large integers, while the later algorithm introduced could be modified by replacing multiplication with addition of points on the elliptic curve mod p (where p is some prime number) (Bernstein & Lange, 2017). The "mod" here refers to the use of modular arithmetic, where a number mod p is equal to its remainder when divided by that number (for example, $7 \equiv 3\ (mod 4)$, since 3 is the remainder when 7 is divided by 4). This method will become particularly effective as quantum computing continues to advance, and is even expected to thoroughly break ECC as a branch of cryptography (Bennett et al., 1997; Bernstein & Lange, 2017). This will be discussed further in later sections of the paper.

Pollard ρ-Method

The Pollard ρ-method is quite popular for large factorizations, and, as with Shor's algorithm, can be modified to implement elliptic curve additions. While this method would still be incredibly tedious on its own, it is possible to run multiple processors in parallel. Since more attempts would be occurring simultaneously, the time needed to break the elliptic curve discrete logarithm problem would decrease significantly for each processor used (Koblitz et al., 2000).

Other Approaches

These are but two of the ways attackers could attempt to break an elliptic curve cryptosystem. Other strategies include using Weil pairings of elliptic curves, J. Silverman's "xedni calculus," and a variant of the Tate pairing (Koblitz et al., 2000).

The ability to exploit side channels of ECC also exists. These attacks are insignificant when systems are sophisticated enough, but still warrant concern when that threshold has not been met. Even then, simple countermeasures such as randomness or "dummy operations" can render these attacks irrelevant (Dhanda et al., 2020, p. 468).

Quantum Cryptography

As quantum computing continues to develop, its applications to the field of cryptography become more feasible. Quantum cryptography is a rather broad field, but its being rooted in the properties of quantum data transmission are quite promising, as it suggests an ability to protect data to a greater extent merely due to how it is transmitted.

Quantum Computing

In contemporary computing, data is stored in bits, and the more well-known binary standard of using 0 and 1 to store all of the information is employed. Quantum computing uses qubits (quantum bits), often small particles such as an atom or photon. The data is stored and read in a similar manner to the way most systems currently look for 0s and 1s, although the quantum system looks for one of two states of the qubit that correspond to that result. A common example is whether a photon's polarization is horizontal, corresponding to 0, or vertical, corresponding to 1 (Bennett & DiVincenzo, 2000; Bruss et al., 2007).

Quantum computing is particularly noteworthy because it is expected to completely outperform any previous system for computations. The power of systems currently in use pales in comparison to the expected strength of quantum systems, and it is only a matter of time before they are widely integrated. While it is expected that quantum computers will develop similarly to the way standard computers have, requiring large amounts of space at first (Gheorghiu et al.,

2018), there will come a time in which the quantum computer has surpassed the modern computer in every conceivable way, as their potential strength is far greater.

Applications to Cryptography

While quantum computing requires further development before widespread use can be effectively implemented, cryptosystems built within quantum methods will have added security in that the nature of quantum computing prevents information interaction without altering that information, thus alerting the two parties attempting to communicate when comparing the correlations of the states of their qubits (Alléaume et al., 2014). By using atoms or light particles to transmit data, which have spin and orientation respectively, any form of tampering can be easily observed. This leads to what is known as the No Cloning Theorem, which simply states, "In a quantum system, information cannot be copied or read by an eavesdropper" (Bruss et al., 2007, p. 11; Kumar & Garhwal, 2021, p. 3831).

Many of the methods listed below take advantage of quantum entanglement, as they rely on the use of entangled states. Quantum entanglement occurs when two particles have many of their physical properties "tied" together, making it so that any action affecting the state of one particle also affects the other, and their states cannot be read as individual particles. Many of the most secure quantum cryptography methods use entangled states, and it can even be described as "the heart of quantum cryptography" (Kumar and Garhwal, 2021, p. 3833).

Methods

Quantum cryptography has a variety of methods. The most well-known system is the BB84 protocol, developed by Charles Bennett and Gilles Brassard in 1984 (hence the name), but a variety of other methods have also been developed. Some of these methods make use of

quantum properties like entangled states, or other mathematical ideas like matrices or continuous variables. One application even uses the properties of quantum cryptography to present a game of chance between the two users with a verifiable winner, rather than relying on whether one party is telling the truth (Bennett & Brassard, 2014).

An important note with quantum methods is that it can be difficult to distinguish orientations associated with the qubits if the systems being used do not have significant variation. Usually, Bob would use either the rectilinear basis, which considers horizontal and vertical orientation, directions 0° and 90°, or the circular basis, with directions of 45° and 135° (Kumar & Garhwal, 2021). While both bases may have a role to play in a particular method, an individual qubit will only ever be measured according to one basis. This is because it would be impossible to reliably distinguish, for example, a 45° orientation from a 90° orientation when correctly and consistently interpreting the states of the qubits is essential for the cryptography (Bennett & DiVincenzo, 2000).

The BB84 Protocol

The BB84 Protocol is a fairly straightforward process. The first party, Alice, sends a qubit to the second party, Bob. For this example, consider the use of polarization of photons with horizontal orientation corresponding to 0 and vertical orientation corresponding to 1. Alice can communicate to Bob through other channels which basis for polarization is being used, and then they can compare measurements to ensure the security of the quantum channel. If Alice sends a test qubit with a horizontal polarization, but it does not reach Bob with that expected polarization, it becomes clear that some form of eavesdropping has occurred, as the polarization has been altered.

This illustrates the core idea of the protocol, but actual practice implements multiple qubits, and the bases by which they are measured are selected at random by Alice. Bob also evaluates each bit by random bases, so approximately half of the bits sent will be evaluated in the same manner by each of them. Both parties would then take half of the remaining bits and ensure that the polarizations match; significant deviation would lead them to conclude the presence of an eavesdropper, while significant agreement (allowing for some degree of error) would show that the remaining private quarter of the original batch of qubits would be safe to use as a key (Bruss et al., 2007; Kumar & Garhwal, 2021).

Other protocols exist that function similarly to the BB84 protocol with some alterations to function. The BBM92 Protocol (Bennett, Brassard, Mermin, 1992) has both Alice and Bob receive their photons from the same source, resulting in a stronger correlation in the absence of an eavesdropper should they both use the same basis for measuring polarization. The B92 Protocol (Bennett, 1992) deviates from standard practice of all of the bases being orthogonal. Instead, Alice would assign, at random, one of two non-orthogonal orientations to 0 and 1, and send them to Bob. Since Bob would measure approximately half of the bits in each basis of orthogonal orientations, he would have certainty for half of each set, which would still amount to half of the total selection of bits received. The two parties could then compare and discard by the same process as in BB84 (Kumar and Garhwal, 2021).

Entangled States

The Ekert 1991 protocol (E91) is the primary example of cryptography using entangled states. The process entails that both parties receive one of two entangled photons, and that their measurements will yield either perfect correlation or perfect anti-correlation in the absence of an

eavesdropper. As with previous methods, Alice and Bob would reveal their measurements, compare results, and be able to discard discrepancies and try again, being able to sacrifice test measurements until a secure channel was established (Kumar and Garhwal, 2021).

Nagata, Diep, and Nakamura (2020) presented a method based on the E91 Protocol. Alice selects a function along which the information is encrypted, and then applies a transformation based on the function to a qubit to create an entangled state. With this information, Bob is then able to extract the function by comparing the final and initial states. Should there be any attempt to eavesdrop, the initial and final states will not match, and Alice and Bob can simply try again with new states and a new function.

A similar protocol presented by Diep, Nagata, and Wong (2020), again based on the E91 protocol, uses entangled states with continuous variables. This strategy follows the same process of selecting a function, generating an entangled state, and enabling Bob to determine the function based on the states. The difference is in the implementation of continuous variables in the entangled states, adding an extra layer of complexity to the encryption.

Other Methods

In addition to these methods, several others exist that take advantage of the properties of quantum cryptography, although they are not as well-known. In some cases, there may be trade-offs between using these methods compared to the more standard methods discussed previously.

The Six-State protocol is a generalization of the BB84 protocol, using six states facing the positive and negative directions of the x-, y-, and z-axes of a Bloch Sphere (Kumar and Garhwal, 2021). A Bloch sphere is a visualization of qubits as points on the surface of a sphere, in which operations are represented as rotations of the sphere (Gheorghiu et al., 2018). This

method can be more secure than BB84 in theory, but runs into implementation issues, as well as requiring Bob to measure the orientation of his photons after Alice has revealed the bases over a public channel, rather than before. Since this occurs after Bob has received his qubits, it requires Eve to rely on guesswork to retransmit any intercepted qubits correctly to Bob, in which case approximately 1/3 of Bob's qubits would become incorrect.

The SARG04 Protocol requires that Alice emit two photons where one would be sent in BB84, and the bases are never revealed. Two additional states would then be transmitted by Alice with openly declared bases for measurement assigned to each. When these are sent, one state will match Alice's declaration, and the other has a 50% chance of not matching the declaration, but the only way to know which is for this to occur, thus signaling to Bob that the correct basis for measuring the original qubits is the one that matched (Kumar and Garhwal, 2021).

Nagata and Nakamura (2018) presented a system utilizing matrices. After outlining an algorithm through which a string of integers can be evaluated with one query, they can use measurement of a sufficiently large quantum state to determine multiple strings at once. In their algorithm, each string is assigned to one column of a matrix, and the quantum state accommodates each row. By combining queries through matrices and quantum cryptography together, this algorithm is able to convey a large array of data with one request in a system.

Strengths

Quantum Cryptography's primary strength comes from its security being rooted in the method by which data is transmitted, rather than the mathematics used to encrypt said data. The algorithms used in the transmission add further security to a process that is already somewhat

difficult to eavesdrop on, rather than being the sole reason the data is protected. As discussed previously, properties like the No Cloning Theorem show that Eve cannot even read the data being transmitted without interfering with the qubits, thus alerting Alice and Bob.

Weaknesses

While the No Cloning Theorem makes it difficult for Eve to interfere with Quantum communications, there are several strategies an attacker might employ to gain access to private information.

Backflash Emissions

One potential threat to quantum systems is the possibility that Eve could learn information by gleaning it from backflash emissions rather than the actual photons being sent. Backflash emissions result when certain systems emit light after detecting a photon. The information this emission could pick up has the potential to allow Eve to learn information about the photons in the receiver without running the risk of tampering with the qubits themselves. While a single backflash would not provide an eavesdropper with a comprehensive breakdown of everything Bob would be receiving, it does present enough risk of information leakage to be a concern, as the possibility does exist for Eve to potentially determine the key being used from pieces of information in the backflash.

Some countermeasures for potential backflash attacks do exist. Firstly, the application of a spectral filter to the receiver would significantly reduce the amount of backflash emissions. Pinheiro et al. state that this reduction would be by a factor of 14. They also discuss a procedure that Bob could carry out to reduce the ability of Eve to exploit the emissions by determining the likelihood of a backflash emission, as well as the reverse transmission efficiency of the photon

receiver, and then adjusting the algorithm and implementing privacy amplification procedures as needed (Pinheiro et al., 2018).

Faked States

Another potential method through which one could eavesdrop on quantum communications is Makarov and Hjelme's faked states attack. While it would be quite difficult for Eve to resend a quantum state without signs of tampering, an eavesdropper could employ a strategy where they intercept the original state and send an entirely new one that Bob could reasonably believe is the original. The new states sent by Eve would be the titular faked states.

For Eve to send these faked states, a tap would need to be inserted somewhere in the system being used for communication. This task becomes more difficult if Eve does not have access to copies of the technology being used by Alice and Bob, there is no opportunity to insert the tap while the quantum channel is not in use, too much time passes before Alice and Bob publicly discuss the states, and/or a continuous monitoring detector is present in Alice and Bob's communication system. Should Eve be successful, even despite any of these factors being present, she would be able to access the entire key (or part of the key, should she be partially successful).

Two main precautions can be taken to mitigate this attack. The first is the implementation of a random number generator to set the number of bases to be detected. The concrete inconsistency would make it more difficult for Eve to reliably sneak alternative qubits in without alerting Alice and Bob. The second, alluded to previously, is the installation of a narrowband filter and monitoring detectors, as they make it much more difficult for light to enter the system from outside sources without being detected (Makarov & Hjelme, 2005).

Timing Side Channels

Another risk that exists with quantum cryptography is the possibility that an eavesdropper may use the time between detections of photons to learn information about the key, since the detections need to be publicly announced for quantum protocols. However, the countermeasures for this attack are fairly simple: The delays must be either standardized or randomized to ensure that detecting abnormalities would be a simple process (Lamas-Linares & Kurtsiefer, 2007).

Other Threats

An assortment of other potential threats to quantum cryptography exist. Adequate protective measures should be taken with regards to photon detectors. The backflash emissions attack has been discussed previously, but they are also vulnerable to attacks based on wavelength dependency, detector control, and efficiency mismatch. Additionally, the system at large could be exploited should information be leaked through separate security concerns, such as a trojan horse attack, or if the system were interfered with through laser seeding or laser damage (Pinheiro et al., 2018).

Furthermore, while it is not necessarily a threat from a malicious party, quantum systems do need to be designed bearing in mind that the surrounding environment could interfere with the transmission of particles (Bennett and DiVincenzo, 2000). While a certain degree of tolerance is technically permitted for effective quantum computation, the risk of unreliable data as a result of measures not taken is one that must be considered when dealing with quantum systems.

Comparisons

Variety of Techniques

Both Elliptic Curve Cryptography and Quantum Cryptography provide their users with a wide variety of algorithms through which information can be transmitted. Quantum Cryptography, being still in its earlier stages, has plenty of time for even more strategies to be developed in addition to those currently devised. Elliptic Curve Cryptography, despite being an older system by comparison, is still having strategies developed as recently as 2021 (Aljamaly & Ajeena). Neither branch of cryptography is too restrictive of its users in terms of the options available for employing their strategies; each has been significantly expanded and bears potential for continued expansion as technological and mathematical understanding improves over time.

Viability

Elliptic Curve Cryptography is the only of the two systems that is consistently viable at a large scale as of the writing of this paper. This is simply because Quantum Cryptography needs more development and implementation to be readily available on such a scale. When this does occur, however, Quantum Cryptography will clearly be the superior choice, as its security has a certainty to it, given the reliance on physics for the protection of the information. Elliptic Curve Cryptography, like its contemporaries, is quite strong, but ultimately relies on an eavesdropper being unable to solve a mathematical problem(s) due to their difficulty. Difficulty is relative, and even luck with regards to trial-and-error is a real factor. While a fortunate guess or an adversary that finds a complex problem simple enough to solve efficiently (or has devised a way to do so with technology) would be a rare occurrence, these are still possibilities that need to be considered.

Longevity

The fatal reality for Elliptic Curve Cryptography in a world that is approaching a more widespread use of quantum computing is the fact that ECC in its entirety will be easily compromised by quantum computation (Bernstein and Lange, 2017). Quantum cryptography methods are able to defend against quantum attacks, but most pre-quantum methods cannot. Those that can require reworks to do so, and at least have to raise their bare minimum complexity, so they will not be as easy to use. Therefore, when the day does come that quantum systems are in widespread use, any party that seeks secure communications will need to have strong quantum cryptographic methods in place to ensure security. Any entity that fails to do so would be completely vulnerable to any quantum-wielding attackers.

Conclusion

Elliptic Curve Cryptography is a technique with many strengths. It is simple to use, with the ability to add more complexity for further security, and it is difficult to crack even in its base form. At this time, it does not present any algorithms that would be easy for an eavesdropper to crack. While some algorithms have been devised that could in theory break an elliptic curve system, the computational strength does not yet exist to apply those algorithms efficiently to a sufficiently complex system, thus usually preserving any elliptic curve method long enough for Alice and Bob to communicate all of the necessary information. Furthermore, the option will always exist to switch between multiple encryptions, so as to increase the amount of time needed for an enemy to crack the system. Frankly, as long as the Discrete Logarithm Problem persists as a strong line of defense for a cryptosystem, ECC will continue to be a viable and effective means of encrypted communication.

Quantum Cryptography, on the other hand, is quite unique in its strengths. The method of transmission implements physics in such a way that there is already significant security without the need to apply any mathematics to the process. As algorithms are added to the process, the security continues to be strengthened. While most quantum methods are in simple or theoretical stages, in accordance with the present development of quantum computing, the more widespread use of quantum systems in the future will make quantum cryptography a viable, even necessary option for secure communications. Those weaknesses that do exist, even theoretically, all have solutions and precautions devised to mitigate or eliminate the threat they pose. Additionally, since quantum computing systems will need more development time before their widespread use and the subsequent implementation of quantum cryptographic systems, there is also more time for more or stronger countermeasures to be developed to known or even yet-to-be-discovered threats.

Ultimately, a day will come when elliptic curve cryptography, alongside many other contemporary methods, becomes totally eclipsed by quantum cryptography. Many of the present weaknesses of elliptic curve cryptography will only become more of a liability as quantum computing becomes more widespread. While the effective use of quantum cryptography methods is not feasible at this time, it will provide a more secure system than has ever existed prior. Ultimately, with all of the benefits of quantum cryptography, it is clear that the focus of research and development in the field of cryptography should be significantly directed towards ensuring the widespread use of quantum methods, both for the ability to have the most secure communications and to be able to crack enemy encryptions with far greater efficiency.

References

Aljamaly, K. & Ajeena, R. (2021). The elliptic scalar multiplication graph and its application in elliptic curve cryptography. *Journal of Discrete Mathematical Sciences and Cryptography*, *24*(6), 1793-1807. https://doi.org/10.1080/09720529.2021.1932896

Alléaume, R., Branciard, C., Bouda, J., Debuisschert, T., Dianati, M., Gisin, N., Godfrey, M., Grangier, P., Länger, T., Lütkenhaus, N., Monyk, C., Painchault, P., Peev, M., Poppe, A., Pornin, T., Rarity, J., Renner, R., Ribordy, G., Riguidel, M., … Zeilinger, A. (2014). Using quantum key distribution for cryptographic purposes: A survey. *Theoretical Computer Science, 560*(1), 62-81. https://doi.org/10.1016/j.tcs.2014.09.018

Bahramian, M. & Hajirezai, E. (2020). An identity-based encryption scheme using isogeny of elliptic curves. *Series Mathematics and Informatics, 35*(5), 1451-1460. https://doi.org/10.22190/FUMI2005451B

Bennett, C. & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science, 560*(1), 7-11. https://doi.org/10.1016/j.tcs.2014.05.025

Bennett, C. H., Bernstein, E., Brassard, G., & Vazirani, U. (1997). Strengths and weaknesses of quantum computing. *Society for Industrial and Applied Mathematics Journal on Computing*, *26*(5), 1510-14. http://dx.doi.org/10.1137/S0097539796300933

Bennett, C. H. & DiVincenzo, D. P. (2000). Quantum information and computation. *Nature, 404*, 247-255. http://dx.doi.org/10.1038/35005001

Bernstein, D. & Lange, T. (2017). Post-quantum cryptography. *Nature, 549*, 188–194. https://doi.org/10.1038/nature23461

Bruss, D., Erdelyi, G., Meyer, T., Riege, T., & Rothe, J. (2007). Quantum cryptography: A survey. *Association for Computing Machinery Computing Surveys, 39*(2), 260-275. https://doi.org/10.1145/1242471.1242474

Dhanda, S., Singh, B. & Jindal, P. (2020). Demystifying elliptic curve cryptography: Curve selection, implementation and countermeasures to attacks. *Journal of Interdisciplinary Mathematics, 23*(2), 463-470. https://doi.org/10.1080/09720502.2020.1731959

Diep, D., Nagata, K. & Wong, R. (2020). Continuous-variable quantum computing and its applications to cryptography. *International Journal of Theoretical Physics, 59*, 3184–3188. https://doi.org/10.1007/s10773-020-04571-5

Gheorghiu, A., Kapourniotis, T., & Kashefi, E. (2019). Verification of quantum computation: An overview of existing approaches. *Theory of Computing Systems, 63*(4), 715-808. http://dx.doi.org/10.1007/s00224-018-9872-3

Koblitz, N., Menezes, A. & Vanstone, S. (2000). The state of elliptic curve cryptography. *Designs, Codes and Cryptography, 19*, 173–193. https://doi.org/10.1023/A:1008354106356

Kumar, A. & Garhwal, S. (2021). State-of-the-art survey of quantum cryptography. *Archives of Computational Methods in Engineering, 28*, 3831–3868. https://doi.org/10.1007/s11831-021-09561-2

Kumari, A., Abbasi, M., Kumar, V. & Khan, A. (2019). A secure user authentication protocol using elliptic curve cryptography. *Journal of Discrete Mathematical Sciences and Cryptography, 22*(4), 521-530. https://doi.org/10.1080/09720529.2019.1637155

Lamas-Linares, A. & Kurtsiefer, C. (2007). Breaking a quantum key distribution system through a timing side channel. *Optics Express, 15*(15). https://doi.org/10.1364/OE.15.009388

Makarov, V. & Hjelme, D. (2005). Faked states attack on quantum cryptosystems. *Journal of Modern Optics, 52*(5), 691-705. https://doi.org/10.1080/09500340410001730986

Nagata, K., Diep, D. N., & Nakamura, T. (2020). Quantum cryptography based on an algorithm for determining a function using qudit systems. *International Journal of Theoretical Physics, 59*(9), 2875–2879. https://doi.org/10.1007/s10773-020-04547-5

Nagata, K., & Nakamura, T. (2019). Quantum communication based on an algorithm of determining a matrix. *International Journal of Theoretical Physics, 58(1),* 247–254. https://doi.org/10.1007/s10773-018-3926-9

Pinheiro, P., Chaiwongkhot, P., Sajeed, S., Horn, R., Bourgoin, J., Jennewein, T., Lütkenhaus, N., & Makarov, V. (2018). Eavesdropping and countermeasures for backflash side channel in quantum cryptography. *Optics Express, 26*(16), 21020–21032. https://doi.org/10.1364/OE.26.021020

Scholl, T. (2019). Super-isolated elliptic curves and abelian surfaces in cryptography. *Experimental Mathematics, 28*(4), 385-397. https://doi.org/10.1080/10586458.2017.1412371