ISSN 2278-3091

Volume 9, No.5, September - October 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse82952020.pdf

https://doi.org/10.30534/ijatcse/2020/82952020

An overview of Quantum Cryptography and Shor's Algorithm

C. H. Ugwuishiwu[1,1], U. E. Orji[1,2], C. I. Ugwu[1,3], C. N. Asogwa[1,4]

[1]Department of Computer Science University of Nigeria, Nsukka, Enugu State, Nigeria,

[1]chikodili.ugwuishiwu@unn.edu.ng, [2]ugochukwu.orji.pg00609@unn.edu.ng, [3]celestine.ugwu@unn.edu.ng,

[4]caroline.asogwa@unn.edu.ng

ABSTRACT

The paper aims to examine the mechanisms of quantum cryptography and review the relationship between quantum and classical encryption schemes. A brief introduction of quantum computation is provided, with a simplified explanation of Shor's Algorithm showcasing the potentials of quantum computation. Related literature such as books, journals, proceedings, lecture notes and webpages on quantum cryptography were reviewed and were sourced from prominent databases like IEEE Xplore, ScienceDirect, and JSTOR. This gave a clearer picture on the mechanisms of quantum cryptography and Shor's algorithm. The authors were able to succinctly describe quantum cryptography, show how encryption is achieved by exploiting the properties of quantum particles, and demonstrated with examples the intricacies with Shor's algorithm. It is expected that interested researchers will be more informed on current research in quantum cryptography and influence potential cryptography scholars to explore further the mechanisms of quantum cryptography, quantum computation, and other principles of the quantum theory.

Key words: Quantum computation, Quantum theory, Shor's Algorithm, cryptography, and Quantum Public Key Distribution

1.INTRODUCTION

Historically in computing science, there has always been an endless battle between code-makers and code-breakers [1]. Creating a perfect encryption method that cannot be broken has been the holy grail of cryptography in classical computing. The difficulty of classical computing in breaking the encryption is attributed to its low computational power [2]. This paper aims to highlight how classical and quantum computers handle encryption/cryptography and other principles behind it. Shor's algorithm was also discussed to appreciate the complexity in the computing power of quantum cryptography. Previous knowledge of Classical computers says that it encodes only 0 or 1 as its data, while a quantum computer is designed to encode data in 1, 0, or in both 1 and 0 (superposition states) [3]. The quantum computers have been touted to have the required huge magnitude of computing power to break the classical computer encryption [2] [4]. Today, classical computers may take longer than the universe's lifetime to crack some classical encryption algorithms. However, with quantum computers, the same algorithm would take only a fraction of the time. In practical estimation, the quantum algorithm would need about the square root of the time taken by the classical algorithm to compute [5]. It is also important to point out that the term quantum algorithm is explicitly used for those algorithms that are quantum in nature or rely on an essential feature of quantum computation including quantum superposition or entanglement etc.

One of the most vital primitive cryptographic scheme available today is the digital signatures. These cryptographic schemes are based on RSA and discrete logarithm assumptions (DSA, ECDSA). With the expected emergence of the quantum computer, none of the above will remain secured, as proven by the seminal work of Shor [6]. Consequently, researchers in the cryptographic world are increasingly focusing their attention on producing Post-Quantum cryptographic schemes.

Thus quantum cryptography and Shor's algorithm could simply be said to be fully dependent on the superposition/entanglement feature of quantum computers.

1.1 A Brief History of Cryptography and Shor's Algorithm

Since 1900 BC, some form of cryptography have been in use for a long time, with its roots traced back to the Egyptian mummy traditions [7]. The purpose has always been to find a secure means of passing messages.

It all started in 1981 by Richard Feynman at MIT, where he proposed a basic model for a quantum computer. Feynman was able to outline the possibility to outpace classical computers exponentially. Since Feynman came up with the quantum concept, lots of researches have been done on the field. As already pointed out, quantum computers are considered the destructor of the present-day classical cryptography [8].

Peter Shor, an American Mathematician while working in Bell Labs, New Jersey in 1994, formulated the Shor's algorithm. The algorithm was designed for integer factorization. Shor proved that a quantum computer when operating optimally (without succumbing to environmental noise or another quantum related interference) could effectively break classical cryptography schemes such as the RSA. A large integer factorization problem has been a major limitation of classical cryptography, but quantum computers take advantage of Shor's algorithm to solve this problem [9].

2.LITERATURE REVIEW

This section deals with relevant researches by scholars who have worked on quantum cryptography. Presumably, this will help researchers in quantum cryptography and its related fields to get clearer views on what quantum cryptography is all about.

2.1 Classical Cryptography

The whole point of cryptography is to conceal the details of a message from intruders and also to verify the accuracy of the message (authentication).

Cryptography has become extremely essential for the protection of our increasingly digitized world. Encryption is the oldest cryptographic technique with confidentiality as its most significant achievement. It has been available for years but mostly used to protect military and governmental communication before the boom in digitalization. Cryptographic hash functions and digital signature schemes are other essential cryptographic techniques in use to ensure data integrity and authenticity [10].

In classical cryptography, the concept involved includes encryption and decryption, where a parameter known as the key is set by the parties involved, thus the introduction of the avatars; Alice = sender and Bob = recipient.

Encryption C = E_(K)(P)

Decryption P = E_(K)^(-1)(C)

E_(K) is called cryptographic system. K as a parameter selects the specific transformation, the parameter is chosen from a keyspace K [11].

2.1.1 Basic Principles of Cryptography and Shor's Algorithm

Classical systems code data in bits while quantum computer systems code data in qubits. Here, it is possible to encode more than two states in a single qubit (this is called superposition) [12].

Consider a four classical bits computer; typically, they can either be expressed as 2^4 or 16, with different combinations. An example is: 0000, 0001, 0010, 0011 – and so on. This can be in any of the 16 possible states. However, a four quantum bits or qubits, in superposition, are designed according to the quantum theory to be in all the 16 possible combinations simultaneously. So with this theory, a 20 qubits register could store a million values in parallel (2^{20} = 1,048,576). It is possible since an atom can exist in two states (superposition) simultaneously, |0> and |1> [12] as shown in figure 1. The two states here represent the two energy levels of an atom. Thus, |0> is the ground state, and |1> is the excited state. It has been demonstrated that a single Qubit represents the superposition of two states, as shown here:

$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Where α and β are the probability of the superposition collapsing to either |0> or |1> when measured [13].

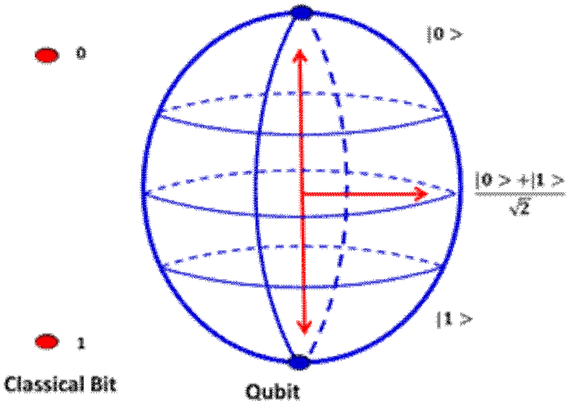


Figure 1: Comparing Classical bit and Qubit Source: [14]

Peter Shor's work on polynomial-time quantum computer algorithms became useful for factoring integers and computing discrete logarithms [15]. Factorization of numbers by Shor's algorithm is shown below:

To find prime factors of the number 15 using Shor's algorithm, a 4-qubit register is needed [16]. For simplicity, a 4-qubit register can be visualized as a 4-bit register of a classical computer, thus, Number 15 in binary is 1111. Thus, a 4-qubit register is used to compute the prime factorization of 15. This type of computation is done in parallel for every value (0-15) that the register can take [17]. It will take thousands or even millions of error-free qubits to break current cryptography schemes in classical computers [2].

2.2 How Classical Computers Handle Cryptography

The need for Privacy while communicating sensitive information has led to the invention of some very fascinating and somehow unusual way of encoding conversations/data from one point to another. For example, during World War II, the Nazis produced a huge machine termed "the Enigma" similar to a typewriter. The device was used to develop a renowned ciphers (encoded messages) of the pre-computer era [18].

While the war was raging, the resistance fighters from the Polish block created a similar machines with full guidelines on the functionalities of the Enigma. But regardless of this enormous feat considering the situation then, it still took a considerable time to decode the messages although, it was eventually broken. This laid the foundation for the continuous circle of encryption and decryption [19]. Soon, public keys became very prevalent in securing data. But here is the catch, cryptology has limitless possibilities for key usage. Cryptology is the study of codes, to find ways to improve secrecy and integrity of data. Public-key and secret-key cryptology are the main two currently in use, and in both of these methods, the sender is identified as Alice while receiver is identified as Bob.

In the public-key cryptology (PKC) method, a user will be asked to choose two interrelated keys, which will then be shared with someone who desires to send a message to him. This entails that even though it is possible that Alice (sender) can send messages to Bob (recipient), the person with access to the key can decode the message. Ideally, even the sender won't know the decryption code.

Here is an analogy to explain this: Consider a mailbox using two keys, one unlocks the front of the box and gives everyone who has access to the key the privilege to deposit mail. While, the receiver has access to the second key that unlocks the back of the mailbox which is used to retrieve messages from the box.

Now lets consider another traditional cryptology method known as the secret-key cryptology (SKC). In SKC, a single key is used by both Alice and Bob to encode and decode the message. Even if the encryption algorithm goes through an unsecure channel, evasdroppers can't decode the message unless they have access to the key **[*00]**.

Here's another analogy to explain further: Consider a mailbox containing a message and key, anyone can access the box but without the key, the message cannot be accessed.

The next approach is OTP (One-Time-Pad). The OTP as an encryption algorithm uses a secret key whose length is as long as the original message being sent. Claude Shannon, in [20], proved that the OTP has absolute security. This random key is only used once, and this becomes a drawback because once the key is used, you would need another one. So, in summary, for classical computers, sending a key over an insecure channel leaves you highly vulnerable to eavesdroppers. If Alice and Bob exchange keys with each other via an insecure channel, there's no clear way to prove if Eve (i.e., an eavesdropper) has made a copy of it or not.

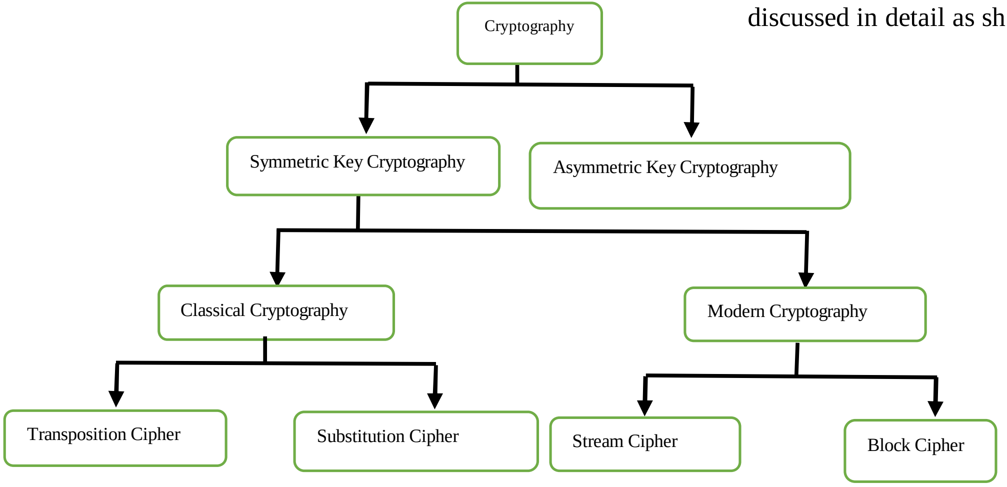


Figure 2: Classical Cryptographic Algorithm [21]

2.3. Fundamental Principles in Classical Computers that Limits its Power to Break Encryption

The major obstacle in breaking today's encryption scheme by classical computers is as a result of the massive size numbers used in the combination of the keys. It was deliberately made to ensure data security. The combination of numbers in modern keys is very complex and intricately designed. For instance, to crack a 128-bit key, the number combination has an exponential power 1038 [20].

You can now imagine the computational power of a system that can get the correct combination and how long it could possibly take. Researchers estimate that it will take a billion computers working in parallel and with each processing as much as a billion calculations per second and will still take a trillion years to crack a key [20]

2.4 Review on Related Literature on Classical Cryptography

Different researches have been published in the field of classical cryptography. In this section, we will present a few of this literature.

In [22], a description of the conventional cryptography fundamentals and its concepts was made.

The book described the basic terminologies and cryptographic schemes, including symmetric and asymmetric cryptography. The authors also highlighted the basic ciphers such as substitution and transposition ciphers, and one-time pads. Information-theoretic approach to cryptography was also talked about.

Authors [10] explained how long-term confidentiality of information had become a major challenge for classical cryptography. This is because of the complexity-based nature of current cryptography methods. This is attributed to the fact that classical cryptographic security is dependent on the intractability of certain algorithms.

Work done in [23] discussed the classical cryptography and techniques connected to it. How to use data string (Key) to secure the transmission of messages between interested parties were discussed. The two main techniques of classical cryptography, namely; Asymmetric and symmetric were also discussed in detail as shown in figure 2.

The paper showed how Asymmetric cryptography uses a key pair to secure data while in symmetric cryptography, the encryption and decryption of data were done using a single key.

In [16], the authors succinctly explained how hash functions, symmetric and asymmetric algorithms are used in modern cryptography. The article analyzed the intrigues and difficulties in factorizing large numbers like in RSA numbers. They also delved into the fundamentals of strong asymmetric ciphers explaining in detail the discrete logarithm problem.

Author in [24] presented a brief introduction to cryptography as a mathematical technique which provides secrecy in data transmission between computers. The early ciphers developed by Julius Caesar and Augustus were also discussed. The author presented the Enigma cipher and the breaking of the Enigma codes, cryptographic systems, and the use of keys, and the advantages and disadvantages of symmetric-key and public-key cryptosystems.

In [25], a comprehensive introduction to modern cryptographic schemes and the necessary mathematical concepts surrounding it was presented. The work discussed encryption and decryption in ciphers. They also compared stream and block ciphers, Data Encryption Standard (DES) and Advanced Encryption Standard (AES), Public-key Cryptography, RSA cryptosystem, and Digital signatures.

Author in [26] explored encryption, decryption, cryptography, and cryptanalysis. The various cryptographic algorithms, including symmetric and asymmetric key cryptography were discussed. The paper also presented RSA algorithm, Hashing function/algorithm, implementation of digital signatures, and possible attacks on cryptography.

2.5 Basic Principles of Quantum Cryptography

Cryptography, in its totality, deals with sending an uninterruptable message from sender to recipient. In layman’s term, cryptography is about three people; Alice (the sender), Bob (the recipient), and Eve (the potential eavesdropper).

In the symmetric system, Alice and Bob share a key, which is random bits enabling the encryption and decryption of the message [27]. In a scenario where Eve intercepts the key, the whole encryption becomes invalidated. So for classical cryptography, safe key distribution is vital, and it is exactly what quantum cryptography addresses.

Quantum cryptography, in reality, has little to do with encryption algorithms and more to do with key distribution via single-photon transmission, making it immune to eavesdropper [28]. Single photons are ideally used to send information in digital form where each photon encodes a 0 or a 1. It is very volatile and hard to detect by eavesdroppers because any stray light can overwhelm the signal [29].

The advances made thus far in quantum science has played a massive role in the emergence of quantum computing and cryptography. Both leveraging on the fundamentals of quantum phenomena like the concept of superposition and entanglement. Superposition describes the ability of a photon to exist in all possible states at the same time (0, 1, 0 and 1), while entanglement describes the linkage of two or more properties of particles intertwined to become one [30].

Unlike in classical cryptography which is focused on the use of mathematical algorithms for data security, the quantum cryptographic scheme harnesses the principles of quantum physics for its data security. This is a safer mission of data communication over unprotected networks [31].

2.6 How Quantum Computers Handle Cryptography

As already mentioned earlier, the only secure way around the problem of encryption algorithms in classical cryptography is through the OTP. However, we have enumerated the possible drawback of that particular method, especially as regards being used only once. Quantum cryptography can handle all issues regarding key distribution by manipulating the features of quantum particles. In this regard, a single photon can represent a qubit, and when one needs to find out the value a qubit carries, you would be required to measure the property of the photon, including its polarization. Now, this is where it gets tricky, measuring the properties of a photon in most cases alters its properties. As such, it becomes extremely difficult for anyone trying to eavesdrop on the transmission since both Alice (sender) and Bob (receiver) can detect any possible changes which arise from the measurement. If an Eve (eavesdropper) tries to measure or copy the key, Alice and Bob will definitely obtain different values for the qubits when they compare them and can discard the Qubit. This ensures that quantum cryptography is for now uncrackable. However, in the future, a method of measuring quantum particles that will not necessarily affect its state may be discovered. Scientists are currently working on this.

2.7 Quantum Public Key Distribution

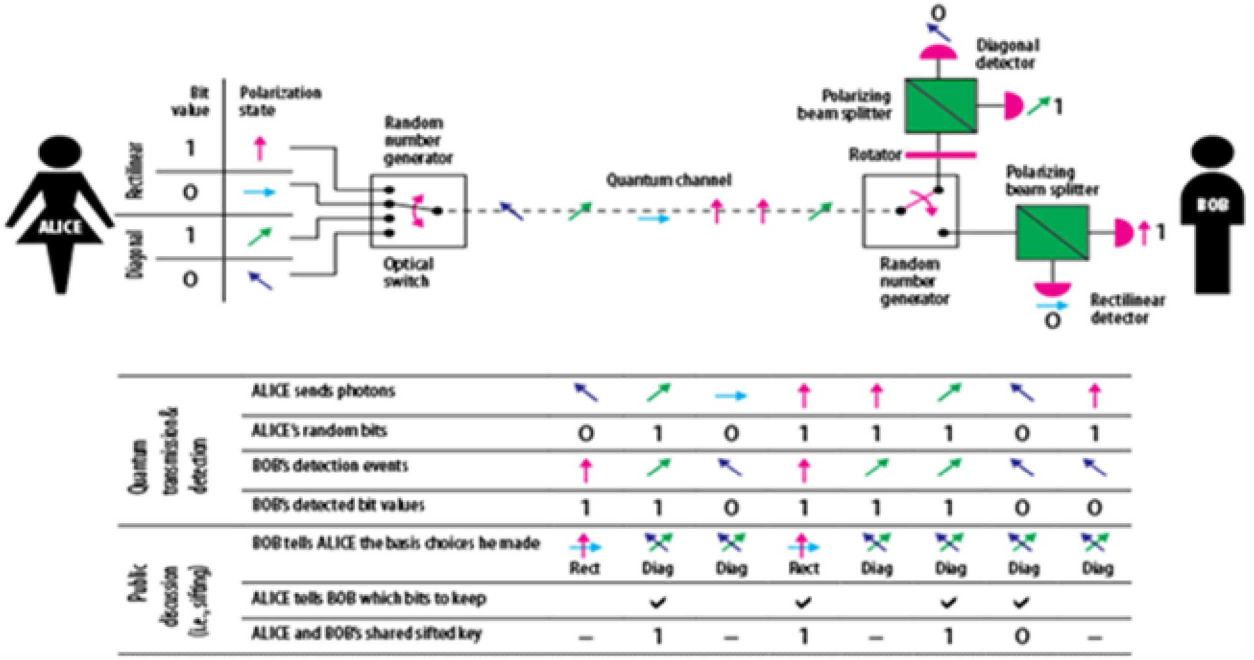
Since it has been established that the most difficult challenge faced by the classical encryption method is that its core architecture relies on the strength of the mathematical computation used to design it, thus, limiting any assumptions on the capabilities of the attacker [32]. Quantum Key Distribution then becomes the shining star to address the challenges faced by classical cryptography using quantum properties to exchange secret information like cryptographic keys. This can then be used to encrypt messages that pass through insecure channels.

Quantum transmission is done through a sequence of polarization bases in the form of rectilinear or diagonal photon positions. A horizontal or 45-degree photon denotes a 0 binary bit while a vertical or 135-degree photon denotes a 1 binary bit [33].

The polarization of light is very efficient for encoding quantum information since light is made up of indivisible particles called photons. Quantum researchers can create photons one-at-a-time and encode quantum bits of information into their polarization. By sending polarization-encoded photons from one person to another, we can build secure quantum networks [34]. Labs studying quantum light can even entangle the polarization of many photons.

The random max of rectilinear and diagonal photons in a quantum transmission means any interference will alter the transmission and stir up disagreements between Alice and Bob on some of the bits as shown in figure 3 [35].

Quantum entanglement and non-locality, a phenomenon that ensures that each particle's quantum state cannot be individually identified, was also discussed. Other important topics from the research paper include; quantum cryptographic constructions, and quantum cryptographic limitations and challenges.



Quantum transmission & detection	ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
	ALICE'S random bits	0	1	0	1	1	1	0	1
	BOB'S detection events	↑	↗	↖	↑	↗	↗	↖	↖
	BOB'S detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made	✛ Rect	✕ Diag	✕ Diag	✛ Rect	✕ Diag	✕ Diag	✕ Diag	✕ Diag
	ALICE tells BOB which bits to keep		✓		✓		✓	✓	
	ALICE and BOB'S shared sifted key	–	1	–	1	–	1	0	–

Figure 3: Quantum Public Key Distribution BB84 protocol [36]

2.8 Review on Related Literature on Quantum Cryptography

This section covers some research papers published on Quantum cryptography.

The paper [35] discussed the properties of polarized photons, which is a key element of a quantum system. Polarized light is generated by sending an ordinary light beam through a polarizing apparatus. Although polarization is a continuous variable; however, the uncertainty principle ensures that no photon can reveal more than one bit about its polarization on measurement. This is one of the reasons why quantum cryptography is highly secured when compared to classical cryptography. In quantum public key distribution, the quantum channel is not directly used to send messages. Instead, it is used to transmit a supply of random bits between users. Then, when investigated subsequently subject to passive eavesdropping, the users can detect with high probability if the original quantum transmission has been disturbed in transit.

In [37], the basics of quantum information in detail, including the unitary evolution and circuits in the linear operation of a quantum system. The quantum no-cloning feature which makes it physically impossible to clone a quantum system.

The authors in [30] discussed the general principles of quantum science and quantum technologies. They explained in detail the principles of quantum cryptography, especially quantum key distribution (QKD), how it works, and its weaknesses. They identified the two primary forms of a quantum communication network; the use of QKD across nodes with fiber connection and then, the "free space" quantum communications via open air. The authors also discussed the advances in the research on "quantum materials" and their potential impact on quantum science.

The current and prospective markets for quantum key distribution (QKD) and related quantum communications technologies was examined in [38]. The work showed how distance impacted the widespread use of QKD and compared the overall security architecture of the quantum system over the conventional classical cryptographic systems. According to the authors, QKD products have been commercialized publicly for over a decade and are valued at $50-500 million annually.

In [39], the authors provided a comprehensive insight into quantum science and cryptography. They started with the origins of cryptography and quantum communications, showed the experimental state of advanced quantum communication with entangled photons, quantum logic using linear optics and quantum state sharing. They also explained further the intrigues of free-space quantum cryptography and then how noise-immune quantum key distribution works.

The authors in [40] experimented on the effect of turbulence on an underwater quantum channel using twisted photons. The aim was to show the feasibility of high-dimensional encoding schemes in comparison with different quantum protocols in an underwater quantum channel. The researchers sent a Gaussian laser beam over a 3m underwater link at a wavelength of 635nm. The result showed that they successfully achieved a positive secret key rate with a 2- and 3-dimensional QKD BB84 protocol.

3. CLASSICAL CRYPTOGRAPHY VS. QUANTUM CRYPTOGRAPHY

Classical cryptographic schemes rely heavily on mathematical algorithms with huge prime numbers that are virtually unbreakable by today's classical computers. These assumption that it is impossible to break the prime numbers used for classical cryptography is its major limitation because theoritically, with the expected speed and superposition feature of quantum computers, the security architecture of classical encryption will crumble when tested on quantum computers in the future.se.

Quantum cryptographic schemes on its part works by transmitting information on an atomic level through photons, where the laws of quantum mechanics guarantee its security [41].

The uncertainty principle guarantees a novel cryptographic phenomenon in an elementary quantum systems that is impossible to replicate in conventional transmission media. In principle, within a quantum communications channel, it is impossible to eavesdrop without being detected because of the high-probability of disturbance when it encounters any external interference while transmitting [35].

Furthermore, quantum and classical cryptography can be compared in terms of the following features:

a) Technological features: For effective transmission of data in a quantum communication system, the ideal distance is 50 Km [42]. However, in classical cryptography, the communication distance may potentially span several million Km. Although, there is a new bitrate record for quantum communciation via QKD, that is, real-time secure keys transmitting continuously at rates exceeding 10 Mb/s [43]. For classical cryptography, the bit rate depends largely on the computational power.

b) Economic features: Quantum Cryptography is currently only suitable for point-to-point connections and is very expensive [44]. On the other hand, classical cryptography can be implemented in software at almost zero cost to the consumers.

c) Application features: Digital signatures reveal the authenticity of digital data to the receiver for classical cryptography. A digital signature assures the recipient that the message was not disrupted in transit [32]. The three main algorithms are key generation, signing, and key verification. But in Quantum Cryptography, algorithms cannot be implemented very easily as it uses quantum mechanism to secure data.

d) Fundamental dimension: In theory, any classical private channels can be easily monitored without the knowledge of the sender or receiver. But, this is difficult in quantum systems because of the volatile nature of the photons [23].

4. SHOR'S ALGORITHM

Prime numbers are, by definition, divisible only by themselves (or the number 1). They are the foundation of the number system. So, when asked the prime factors, or multipliers, for the number 15, almost every student with basic mathematical background knows the answer to be; 3 and 5 by memory. However, a larger number, such as 91, might call for some pen and paper before one could solve it. Also, a larger number, like 232, can (and has) taken scientists two full years to factor, even with hundreds of high-speed classical computers operating in parallel. Most encryption schemes like credit cards, state secrets, and other confidential data are based on the difficulty in factoring these numbers [45]. For example, in 2016 the RSA-220 which is 220 digits long was factored with significant computer resources [46]. Theoretically, a single qubit computer can easily crack this problem, by using hundreds of atoms, in parallel, to quickly factor the RSA-220 and other huge numbers.

Peter Shor, in 1994, came up with a quantum algorithm that was able to compute with a high-level of efficiency the prime factors of huge numbers that previously impossible for any classical supercomputer [47].

The basic idea of Shor's algorithm is the process of period-finding using the Quantum Fourier Transform (QFT). The QFT takes some function f(x) and figures out the period of the function [48].

Shor's algorithm is given as follows:

1. First, a random positive integer $m < n$ is chosen, then the gcd(m, n) is calculated in polynomial time using the Euclidean algorithm. If gcd(m, n) $\neq 1$, the prime factor of n has been found, and the problem is done. But, if gcd(m, n) = 1, then proceed to step 2.
2. A quantum computer is then used to get the unknown period P of the sequence and is given as follow; x mod n, x2 mod n, x3 mod n, x4 mod n, ... 4.
3. To proceed, if P is found to be an odd integer, step 1 is repeated. But, if P is an even integer, we proceed to step 4. Since the period P is even, $(m^{P/2}-1)(m^{P/2}-1)=m^{P}-1=0$ mod n
4. The next step is to check if $m^{P/2} + 1 = 0$ mod n, and if so, step 1 is repeated. However, if $m^{P/2} + 1 \neq 0$, then proceed to step 5.
5. Finally, *to compute d* = gcd($m^{P/2}$ - 1, n), we use the Euclidean algorithm, and since $m^{P/2} + 1 \neq 0$ mod n was proven in step 4 above, we can also show that d is a significant prime factor of n.

An example to illustrate Shor's algorithm is as follows:

Below is an example of how n = 91(=7*13) can be factorized using Shor's algorithm:

1. A random positive integer m = 3 is chosen since gcd (91,3) =1
2. The period P is given by:

$$f(a)=3a \bmod 91$$

Shor's algorithm is used to find the period P, on a quantum computer, i.e., P = 6. Since the period P is even, we proceed to step 4.

3. Since the equation does not equal 0 mod 91, we proceed to step 5.

$$3^{P/2}+1=33+1=28\neq 0 \bmod 91$$

4. See below:

$$d=gcd(3^{P/2}-1, 91)=gcd(33-1, 91)=gcd(26,91)=13$$

Through careful calculation and the use of a quantum computer, the significant prime factor of d = 13 was found of n = 91 [49].

Note: So far, many researchers in quantum science have tried to implement Shor's algorithm with quantum systems; however, none have been successful in a scalable way with more than a few quantum bits [50].

5. AREAS OF APPLICATION OF QUANTUM CRYPTOGRAPHY

The powers of quantum computers and their ability to perform complicated tasks have been discussed in this work. But is it currently commercially available in the market? The simple answer is, no, it is still a work in progress. Furthermore, the successful implementations of these application areas may depend on the use of a hybrid platform that combines the powers of classical and quantum computing both safely done in a cloud environment to achieve the best of both worlds [51].

So here is a list of some quantum cryptography application areas:

1) Computational Chemistry: When the right catalyst with which a new material or an existing one can efficiently be improved upon is developed, many problems in material science can easily be solved. So far, classical computers are being used to simulate the chemical interactions, but sometimes, the problem might become impossible to solve classically. Richard Feynman researched how a quantum computer can be useful in simulating the quantum mechanical processes [51].

Below are examples of some crucial problems that when solved could be impactful:

i) The current Haber process in the production of ammonia used in fertilizers needs

ii) To achieve room-temperature superconductor, we need to find new and sustainable materials.

iii) Finding a catalyst that can improve the efficiency of carbon sequestration.

iv)Today's lithium-ion batteries need urgent improvement,

we need new battery chemistry for improved performance [52]

Circuit, Software, and System Fault Simulation: Developing a large software program usually involves millions of lines of code or large Application-Specific Integrated Circuit (ASIC) chips that have billions of transistors. Checking for correctness in this scenario with a classical computer is usually very expensive and challenging. Error detection and management is vital. The costs of an error can be very high in terms of cost or even saving lives. Using quantum computing for these simulations can potentially provide much better coverage and save time [52].

2) Quantum Internet: The first demonstration of Quantum Internet was between the Chinese Academy of Sciences and their Austrian counterpart. The institutions experimented with intercontinental quantum communications, targeting the establishment of a secure video conference between them. They succeeded in sending the first packets of photons 1200km from the ground to the Chinese Micius satellite. The satellite passed over China, and relayed the packets to Europe. This established a secure communication pathway between Austria and China through fiber optics for an impressive distance of 7600km. This laid the ground for a future quantum internet [13].

2) Swiss Secure Balloting: Switzerland pioneered electronic voting over the internet. The Swiss are renowned as the first country that used a quantum cryptographic scheme to secure their electronic ballots. They used quantum cryptographic scheme to secure the link between their central ballot-counting station and the government's data centers over fiber-optic channels. The encryption boxes used quantum cryptographic technology for secret keys exchange and Triple-DES for point-to-point connection security. The machine had encrypting bit rate of 1Gbps. A significant downside is that the hardware used has a 50-mile transmission distance limit after which the protons performing the encryption began to degrade [53].

6. DISCUSSION

In this paper, the paper has been able to simplify and introduce readers to classical and quantum cryptography and the basic principles surrounding cryptography. Some relevant researches done in the various fields of classical and quantum cryptography were reviewed. The paper is intended to be a motivating factor and a good foundation for beginners in the field of quantum cryptography to explore further into quantum science.

7. CONCLUSION

More than ever, the demand for privacy and data security is high, especially with the prevalence data breach in government and organizational databases worldwide. Quantum computers and Shor's Algorithm signals even more danger for today's cryptographic systems. This has increased the interest of researchers in Quantum cryptology to find ways to guarantee data security.

REFERENCES

[1] Ed. Urie, "Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union. By Stephen Budiansky. New York, NY. Borzoi Book, Published by Alfred A. Knopf, Penguin Random House, New York, 2016.." Journal of Strategic Security 10, no.3 (2017):94-95. DOI: http://doi.org/10.5038/1944-0472.10.3.1641 Accessed on: Aug. 23, 2019. [Online] Available at: http://scholarcommons.usf.edu/jss/vol10/iss3/7

[2] R. De Wolf, "The potential impact of quantum computers on society." Ethics Inf Technol 19, 271–276, 2017. Accessed on: Aug. 23, 2019. [Online] Available at: https://doi.org/10.1007/s10676-017-9439-z

[3] D. Maslov, Y. Nam, & J. Kim, "An outlook for quantum computing [point of view]." Proceedings of the IEEE, 2018, 107(1), 5-10.

[4] J. P. Aumasson, "The impact of quantum computing on cryptography." Computer Fraud & Security, 2017(6), 8-11.

[5] A. Bhalla, E. Kenneth, and H. Matthew. "Quantum Computing, Shor's Algorithm, and Parallelism." Accessed on: Aug. 23, 2019. [Online] Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.1823&rep=rep1&type=pdf

[6] JF. Biasse., G. Micheli, E. Persichetti, P. Santini "LESS is More: Code-Based Signatures Without Syndromes. In: Nitaj A., Youssef A. (eds) Progress in Cryptology - AFRICACRYPT 2020. AFRICACRYPT 2020." Lecture Notes in Computer Science, 2020, Vol. 12174. Springer, Cham

[7] S. Huzaifa "A Brief History of Cryptography," Jan. 2, 2019, Accessed on: May. 13, 2019. [Online]. Available: https://access.redhat.com/blogs/766093/posts/1976023

[8] Mavroeidis, Vasileios, Kamer Vishi, Mateusz D. Zych, and Audun Jøsang. "The Impact of Quantum Computing on Present Cryptography," International Journal of Advanced Computer Science and Applications, 2018, Vol. 9, No. 3.

[9] J. Norman. Formulation of Shor's Algorithm for Quantum Computers, Apr. 30, 2020, Accessed on: June. 13, 2020. [Online]. Available: http://www.historyofinformation.com/detail.php?id=3877

[10] J. Buchmann, J. Braun, D. Demirel, M. Geihs. "Quantum cryptography: a view from classical cryptography." Quantum Science and Technology. 2017 May 25;2(2):020502.

[11] W. Diffie, M.E. Hellman. "Privacy and Authentication: An Introduction to Cryptography," in Proc. IEEE, Vol. 67(3) Mar 1979, pp 397-427

[12] T. Li, & Z. Q.Yin. "Quantum superposition, entanglement, and state teleportation of a microorganism on an electromechanical oscillator." Science Bulletin, 2016, 61(2), 163-171.

[13] Nils Jacob Sand. "Introduction to Quantum Cryptography," Nov. 23, 2018. Accessed on: May. 13, 2019. [Online]. Available: https://www.norwegiancreations.com/2018/11/introduction-to-quantum-cryptography/

[14] Hussain, Zahid. "Strengths and Weaknesses of Quantum Computing." International Journal of Scientific and Engineering Research. 2016, Vol. 7

[15] M. Ekerå. "Revisiting Shor's quantum algorithm for computing general discrete logarithms." Accessed on: Aug. 13, 2019. [Online]. Available: arXiv preprint arXiv:1905.09084

[16] V. Mavroeidis, K. Vishi, M.D. Zych, & A. Jøsang. "The impact of quantum computing on present cryptography." Accessed on: May. 13, 2019. [Online]. Available: arXiv preprint arXiv:1804.00200

[17] S. Bone and M. Castro. "A Brief History of Quantum Computing," Surveys and Presentations in Information Systems Engineering (SURPRISE), vol. 4, no. 3, pp. 20–45, Accessed on: Aug. 13, 2019. [Online]. Available: http://www.doc.ic.ac.uk/∼nd/surprise 97/journal/vol4/spb3/

[18] L. Andrew. "Breaking Germany's Enigma Code." April 2011; Accessed on: July. 13, 2020. [Online]. Available: http://www.storytellingworld.com/33669/EnigmaMachineWWIIShtr.pdf

[19] J. CLARK. "How Quantum Cryptology Works," Oct. 23, 2007. Accessed on: May. 13, 2019. [Online]. Available: https://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology1.htm

[20] C. E Shannan. "Communication Theory of Secrecy Systems," Bell System Technical Journal, Oct. 1949, Vol. 28-4, pp. 656-715,

[21] Shashank. "What is Cryptography? – An Introduction to Cryptographic Algorithms," May, 2020. Accessed on: July. 13, 2020. [Online]. Available: https://www.edureka.co/blog/what-is-cryptography/

[22] I.B. Djordjevic. "Conventional Cryptography Fundamentals." In: Physical-Layer Security and Quantum Key Distribution. Springer, Cham. 2019, pp 65-91.

[23] Patil, Pooja Anil, and Renuka Boda. "Analysis of Cryptography: Classical versus Quantum Cryptography." International Research Journal of Engineering and Technology (IRJET) 2016, Vol. 3, no. 05.

[24] G. O'Regan. "Cryptography. In: Guide to Discrete Mathematics." Texts in Computer Science. Springer, Cham, Accessed on: Aug. 13, 2019. [Online]. Available: https://doi.org/10.1007/978-3-319-44561-8_10

[25] C. Paar, J. Pelzl. "Introduction to Cryptography and Data Security." In: Understanding Cryptography. Springer, Berlin, Heidelberg; Accessed on: Aug. 13, 2019. [Online]. Available: https://doi.org/10.1007/978-3-642-04101-3_1

[26] U.H. Rao, U. Nayak, "Cryptography." In: The InfoSec Handbook. Apress, Berkeley, CA; Accessed on: Aug. 13, 2019. [Online]. Available: https://doi.org/10.1007/978-1-4302-6383-8_8

[27] M. Abadi, & D. G. Andersen. "Learning to protect communications with adversarial neural cryptography." Accessed on: Aug. 13, 2019. [Online]. Available: arXiv preprint arXiv:1610.06918

[28]M. Brooks. "Quantum computing and communications;" Springer-Verlag London Limited, 1999, PP. 87-93.

[29] T. B. Tentrup, T. Hummel, T. A. Wolterink, R. Uppu, A. P. Mosk, & P. W. Pinkse, “Transmitting more than 10 bit with a single photon.” Optics express, 2017, 25(3), 2826-2833.

[30] E. Kania, and J. Costello. “QUANTUM HEGEMONY?: China’s Ambitions and the Challenge to U.S. Innovation Leadership,” The Second Quantum Revolution. Center for a New American Security, 2018, pp. 3–5, Accessed 16 July, 2020. [Online]. Available: www.jstor.org/stable/resrep20450.5.

[31] K. Crane, L. Joneckis, H. Acheson-Field, I. Boyd, B. Corbin, X. Han, & R. Rozansky. “Assessment of the Future Economic Impact of Quantum Information Science”. Institute for Defense Analyses. (pp. 33-42, Rep.) Accessed 16 July, 2020. [Online]. Available: doi:10.2307/resrep22837.6

[32] T.Y. Wang, X.Q. Cai, Y.L. Ren, R.L. Zhang. "Security of quantum digital signatures for classical messages." *Scientific reports* 5 (2015): 9231.

[33] Quantum-Safe Security Working Group. What is Quantum Key Distribution? Accessed on: May. 13, 2019. [Online]. Available: https://www.quintessencelabs.com/wp-content/uploads/2015/08/CSA-What-is-Quantum-Key-Distribution-QKD-1.pdf

[34] J-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens. "Robust polarization-based quantum key distribution over a collective-noise channel." *Physical review letters* 92.1 (2004): 017901.

[35] C.H. Bennett, G. Brassard. “Quantum cryptography: Public Key Distribution and coin tossing,” Theoretical Computer Science 560. 2014, P. 7-11.

[36] Sophia Antipolis. “BB84 PROTOCOL,” May. 2, 2015, Accessed on: May. 13, 2019. [Online]. Available: http://physique.unice.fr/sem6/2014-2015/PagesWeb/PT/Tomographie/?page=bb84

[37] Broadbent, Anne, and C. Schaffner. "Quantum cryptography beyond quantum key distribution." Designs, Codes and Cryptography 78, 2016, no. 1: 351-382.

[38] Crane, Keith W. “Quantum Communications.” Institute for Defense Analyses, Assessment of the Future Economic Impact of Quantum Information Science, 2017, pp. 33–42, Accessed 16 July, 2020 Available: www.jstor.org/stable/resrep22837.6

[39] V. Sergienko Alexander. “Quantum communications and cryptography.” CRC press, 2018.

[40] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, E. Karimi. "Quantum cryptography with twisted photons through an outdoor underwater channel," Opt. Express 26, 2018, 22563-22573.

[41] Qi Bing, Qian Li, Lo Hoi-Kwong. "A brief introduction of quantum cryptography for engineers," Book Chapter, Publisher: arXiv 2010.

[42] M. Lucamarini, Z. L. Yuan, J. F. Dynes. “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters.” *Nature* 557, (2018) 400–403. Accessed on: July. 13, 2020. [Online]. Available: https://doi.org/10.1038/s41586-018-0066-6

[43] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes. A. Murakami, M. Kujiraoka. "10-Mb/s quantum key distribution." Journal of Lightwave Technology. 2018 Aug 15;36(16):3427-33.

[44] K. Azuma, K. Tamaki, W.J. Munro. "All-photonic intercity quantum key distribution." Nature communications. 2015 Dec 16;6(1):1-6.

[45] “Quantum cryptography and the future of security,” Oct. 8, 2018, Accessed on: May. 13, 2019. [Online]. Available: https://www.wired.co.uk/article/quantum-cryptography-and-the-future-of-security

[46] Z. Bernard. “*A First Introduction to Quantum Computing and Information*.” Springer International Publishing, 2018.

[47] J. BARCAN. "Quantum code cracking creeps closer." IEEE SPECTRUM (2000).

[48] P. Gokhale. “How does Shor's algorithm work in layman's terms?” Nov. 16, 2015, Accessed on: May. 13, 2019. [Online]. Available: https://www.quora.com/How-does-Shors-algorithm-work-in-laymans-terms

[49] D. Krambeck, “Fundamentals of Quantum Computing” Aug. 06, 2015, Accessed on: May. 13, 2019. [Online]. Available: https://www.allaboutcircuits.com/technical-articles/fundamentals-of-quantum-computing/

[50] T. Monz, D. Nigg, E.A. Martinez, M.F. Brandl, P. Schindler, R. Rines, S.X. Wang, I.L. Chuang, and R. Blatt. “Realization of a scalable Shor algorithm.” *Science*, 2016, *351*(6277), pp.1068-1070.

[51] R.P. Feynman. “Simulating physics with computers.” Int J Theor Phys 21, 1982, 467–488. Accessed on: Aug. 19, 2019. [Online]. Available: https://doi.org/10.1007/BF02650179

[52] “The Best Applications for Quantum Computing,” Accessed on: May. 13, 2019. [Online]. Available: https://quantumcomputingreport.com/the-best-applications-for-quantum-computing/

[53] Lester Houston III. “Secure Ballots Using Quantum Cryptography,” *Dec. 2, 2007,* Accessed on: May. 13, 2019. [Online]. Available at: https://www.cse.wustl.edu/~jain/cse571-07/ftp/ballots/index.html