QATAR UNIVERSITY

COLLEGE OF ENGINEERING

QUANTUM KEY DISTRIBUTION WITH APPLICATION TO IOT SECURITY

BY

HASAN ABBAS JOLAN AL-MOHAMMED

A Thesis Submitted to

the College of Engineering

in Partial Fulfillment of the Requirements for the Degree of

Masters of Science in Computing

June 2021

COMMITTEE PAGE

The members of the Committee approve the Thesis of
Hasan Abbas Jolan Al-Mohammed defended on .

_____
Dr. Elias Yaacoub
Thesis/Dissertation Supervisor

_____
Dr. Mohamed Abdallah
Committee Member

_____
Dr. Noor Al-Maadeed
Committee Member

_____
Dr. Jamil Renno
Committee Member

Approved:

_____
Khalid Kamal Naji, Dean, College of Engineering

ABSTRACT

AL-MOHAMMED, HASAN , ABBAS., Masters : June : [2021:], Masters of Science in Computing

Title: Quantum Key Distribution with Application to IoT Security

Supervisor of Thesis: Elias Yaacoub.

The Internet of Things (IoT) connects billions of machines that can interact with each other. IoT is one of the fastest-growing areas in the history of computing, and will continue in this direction in the 6G era. New security problems have been raised, however, for implementing protection mechanisms for IoT devices such as encryption, authentication, and so on, is inefficient, due to their inherent flaws. In fact, Classical cryptographic technology in use today is based on the hardness of certain numerical methods, such as integer factoring or the problem of discrete logarithms. However, because these problems are usually not known to be challenging to a malicious entity with quantum computing capability, the resulting cryptosystems are theoretically insecure. Therefore, a new method of protecting IoT devices needs to be sought. Quantum security depends on the natural physical phenomenon (quantum mechanics) and offers an appropriate and powerful security technique. This thesis suggests a new approach for simulating the quantum key distribution between IoT devices and a server to encrypt the data sent to the server. It also demonstrates the simplicity of this new method, and its efficiency in producing a quantum key distribution (QKD) simulation. In addition, it describes the use of the final length key for symmetrical security for IoT devices. Moreover, the simulation of the attacker between the server and IoT devices is performed, and two machine

learning techniques were applied for detecting an attacker relying on the final quantum key length, even though the effect of that attacker on the quantum key length was within the acceptable threshold range.

DEDICATION

To my father who taught me a lot, to my family on those hard days, *at the end for that person, who I cannot see but I always feel his hands around me.*

ACKNOWLEDGMENTS

To my supervisor, Dr. Elias who supported me in this difficult topic and made it easy, for his patience, guidance, and continuous support, to prof. Mohsen Guizani the first lecturer who encouraged me to deep dive into quantum worlds.

Furthermore, This research was jointly supported by Qatar University and IS-Wireless - IRCC Grant no. IRCC-2021-003. The findings achieved herein are solely the responsibility of the author.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

With the implementation of 5G networks in full effect, a study has started to concentrate on 6G mobile cellular systems. Keeping up with the tradition of a new generation of cellular networks every 10 years or so, it is expected that the 6G infrastructure will be standardized with implementations beginning before 2030. As it always takes more than ten years for a modern invention to see the market day as it always takes over ten years for emerging technologies to see the market light of day, it is time to start research into new technology components for 6G. The Internet of Things (IoT) connects billions of machines that can interact with each other. IoT is one of the fastest-growing areas in the history of computing, and will continue in this direction in the 6G era[1], [2].

Quantum communication involves sending the states of the Quantum bit between two places (whatever the distance between them since they have entanglement for more see section 1.1) via quantum channel. Quantum communication entails three main phases: (i) The original classical information encoding to Quantum bit states, (ii) transmission of the Qubit states via Quantum channel which could be either optical fiber or free space and this depends on the distance of the two nodes and the repeater used, (iii) and detection at the receiver side that detects the Qubit and encodes it to the classical bit by using quantum measurement [3], [4]. Figure 1 illustrates encoding the classical information (symbol A) to the quantum states, the initial classical-quantum mapping to the quantum bit inside classical medium where qA is the quantum states that represent the classical information, qA mapping to q'A inside the quantum channel, where q'A is corrupted state of qA. Then the quantum state decoding to a classical information[4][5].

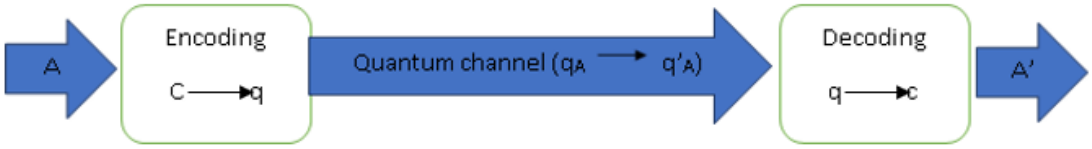


Figure 1: short distance quantum communication.

Fiber-to-Home networks constitute a fundamental broadband segment with the required potential to match the huge capacity of transport networks with the next generation communication demands [6]. Due to photon loss in fiber communication (long distance more than 500km), a quantum repeater must be used. Fig.2 illustrates the communication between two nodes for long distance by using quantum repeater. In Fig. 2, nodes are network entities, stations are the source and destination of information.[4],[7], [8].

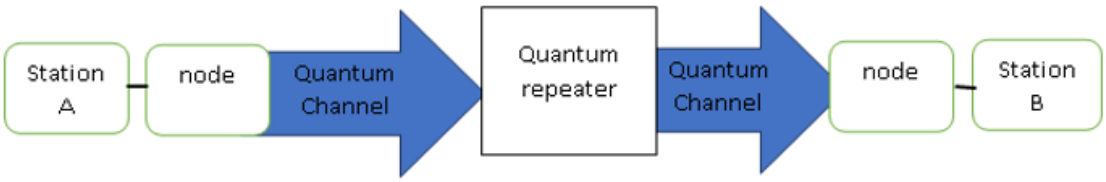


Figure 2: Long-distance communication chain with repeater.

Quantum communication is expected to be better than the classical one whether the communication model has error or it is error-free [9]. According to the studies of the Delft research academy and many other researches in the worldwide institutes, they found that the specifications of quantum communication can build important and powerful applications [4]. However, because of the Qubit type which uses the photon to send the information, the photon can be lost in the channel for the long distances between the sender and the receiver in optical medium. One of the main challenges for the quantum Qubit is the long distances while sending the information.

There are promising solutions that have been proposed to solve this issue either

by using satellite to send the Qubit via space-based link between two nodes or by extending the communication between them by using repeater [10],[11]. In[12], the authors used multiplexed atomic quantum memories by converting the spin-wave that can enhance the established quantum entanglement then enhance the communication of the network (for long-range communication). Also, in [13], the authors proposed wireless quantum multi nodes by storing quantum particles then distributing individually, the information transmitted via intermediate nodes. Moreover, in [14], the authors used a wavelength division multiplexing scheme for classical signals in seven core fiber and quantum signals to carry quantum key distribution (QKD) in one outer core to be used for the quantum channel.

The quantum optical sensing technique used quantum illumination by which an entangled source is browbeaten for improving the detection for the object that has low-reflectivity with high bright thermal background [15]. It is an extension of traditional radar which takes the potential of breakthrough of the limit of conventional radar detection performance [16]. In [17], the authors take advantage of the recent advance in the field of microwave superconducting circuits by proposing a novel microwave quantum-enhanced backscattering system using quantum physics (quantum illumination).

1.1 Quantum mechanics characteristics

It should be recognized that after 1927, many, perhaps even a good number, of physicists gave up the view that quantum mechanics' basic ontology is fundamentally conventional.

In other words, this view stated that physical reality is based on scientifically true, counterfactually defined, uniquely spatiotemporally defined, local, complex

entities with particular valued properties, and that 'quantum' action usually arises as a result of our own ignorance of such entities in theory [18].

1.1.1 Quantum entanglement

In quantum mechanics, entangled particles remain connected so that actions performed on one affect the other, even when split by great lengths. Albert Einstein named the phenomenon "spooky action at a distance." The laws of quantum physics claim that an unnoticed photon occurs concurrently in all potential states, but experiences only one state when detected or measured. Here, spin is defined as a rotation axis, but real particles do not rotate. Entanglement happens as a pair of physically interacting particles, such as photons. A laser beam shot through a certain form of crystal may cause the splitting of individual photons into pairs of entangled photons. A wide distance, hundreds of miles, or even more, can distinguish the photons. Photon A takes on an up-spin state when detected. Entangled Photon B takes up a state relative to that of Photon A, while now far apart (in this case, a down-spin state) [19].

It forms a relationship between the quantum framework and distinguishable parts that surpasses all previously thought to be feasible. It appears that this way of connecting the subsystems such that the complete framework's outcome state is not able to be communicated as a coordinate of other states of the framework' parts. Due to this ensnared state of the quantum framework, the activities on one side of the subsystem will be performed with side effect on the other side of the subsystem even though that performance of the subsystem was not accurately acted. Furthermore, this way of isolating the sub-system regardless of the separated distance will continue this type of traps. This indicates to completely unreasonable questions, as Einstein called

“spooky activity at a distance”, but the advantages is the memory register [20] such as in the quantum computer communication.

1.1.2 No-cloning (cannot copy a quantum bit).

The no-cloning property is one of the fundamental and characteristic differences between classical and quantum facts. This notes that there is no way to design an apparatus capable of taking as input a general quantum state and returning the original state as output plus a copy of any of the information in it. In fact, though keeping the originals intact, it is not feasible to create perfect copies of all the input states. A closely related fundamental fact is that a commuting set of observables can be measured by the apparatus, but that the details in the original state found in the relative phases of the respective spaces must then be discarded [10], [21].

A logical case could be made for the probability of faster-than-light transmission if photons could be cloned. It is well known that for many inseparably correlated Einstein-Podolsky-Rosen photon pairs, if a polarization calculation (i.e. vertical versus horizontal) has been done by an observer on one of the pair's members, the other, which may be far away, can be considered as having the same polarization for all purposes of prediction.

If this second photon could be repeated and its correct polarization determined as before, it would be possible to decide if the first photon, for example, was subjected to linear or circular polarization measurements. Throughout this scenario, by encoding his message into his preference of measurement, the first observer would be able to relay information faster than light. The real impossibility of cloning photons therefore forbids this device from super-luminal contact. A general quantum correlation is that such a mechanism would malfunction for whatever reason,

considering the well-established nature of long-range quantum correlations and the effects of quantum mechanics [22].

1.1.3 Uncertainty principle (Heisenberg's uncertainty principle).

One of the most essential principles in the field of quantum mechanics is the Instability Theory suggested by Heisenberg which exhibits a significant and consistent distinction from its classical equivalent. The theory of uncertainty clearly sets a lower limit on a quantum framework for calculating the measurement effects for two arbitrary conflicting observables. A fundamental limit to the precision in which, from the initial conditions, the values for specific combinations of a particle's physical numbers, such as, position, a and momentum, b, can be predicted [23].

$$\Delta a \Delta b \geq \frac{h}{4\pi} \tag{1.1}$$

Δa is uncertainty in position.

Δb *is* uncertainty of momentum

$h =$ Planck's constant.

1.2 quantum communication based on the nodes' connectivity.

The quantum communication relies on photons for sending and receiving. The photons will lose power and need a repeater for long distance. In the quantum universe, this is different from the classic one, as the photons will not copy to resend it, so it should be a special type of repeaters to send the photons.

This corresponds to a situation when two nodes connect or communicate with each other such as user to the bank server. The repeater is used to make the photon

travel for long-distance, to make entanglement between two nodes, the repeater put in distance between two nodes then node 1 sends a Qubit(photon), same for node 2 which sends a photon inside the repeater to make the entanglement; after that the whole path between the two nodes will be entangled and the two nodes can communicate or used for security login server-node connection. This method is implemented by using guided medium (fiber optic), and it is suggested in [4].

Also, in a free space medium, the repeater sometimes is the quantum key maker and distributor by generating two or more entanglement photons then distributing them into two nodes and these nodes can communicate. This approach depends on Qubit generation then sending the Qubits by reflecting them in a mirror then send using the telescope to node1. Node 1 receives the Qubit also, by telescope then directs it to the node, with the same procedure being done at node 2. After that, all entangled photons can communicate or send or receive without any need for a medium like fiber optic[24], [25], see Figure 3 [11].

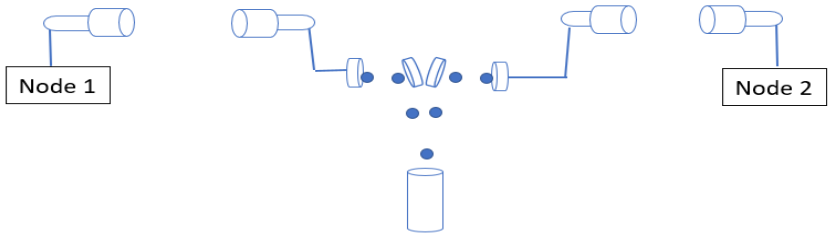


Figure 3:quantum repeater for long-distance relay on free space medium. [11]

1.3 Quantum computing as emerging technology.

Based on Moore's law, the classical physics-based technology may have met its limits, and the electronic transistor on a chip possibly so small (so tiny scale) that we will see the age called "Quantum Era." Quantum technologies are now highly emerging area [26]. Quantum computers depend on the Qubit for their strength. A traditional bit can only store a single value either “0” or “1”, but the Qubit can store

several states of value, which is known as superposition (“0” and “1” at the same time). As a result, the Quantum computer's entire design and architecture is based on handling, measuring, manipulating, and managing of the Qubit [27]. All these factors have contributed to quantum computing being one of the emerging technologies; Gartner's Hype included quantum computing among new technologies in 2011. The most famous emerging technologies in 2011 are depicted in Figure (4). Quantum computing became further trending than the 5G technology in 2018, as shown in Figure (5) that illustrates the trending in 2018 technologies.

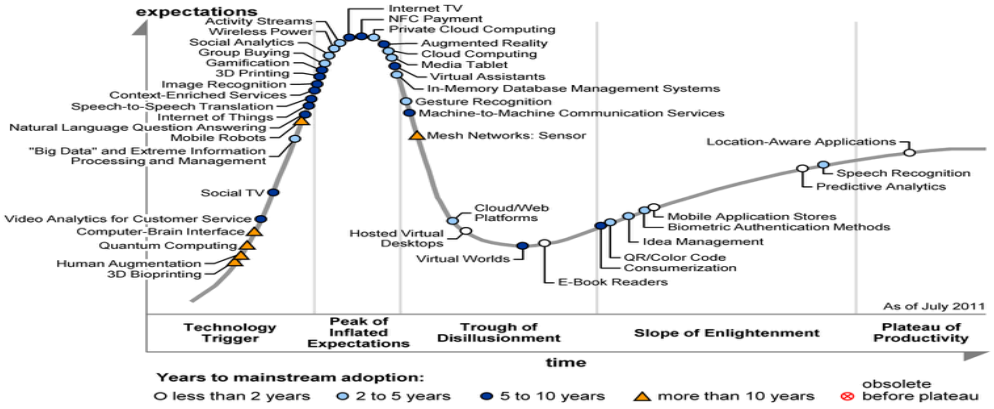


Figure 4. The arising technology in 2011 [27].

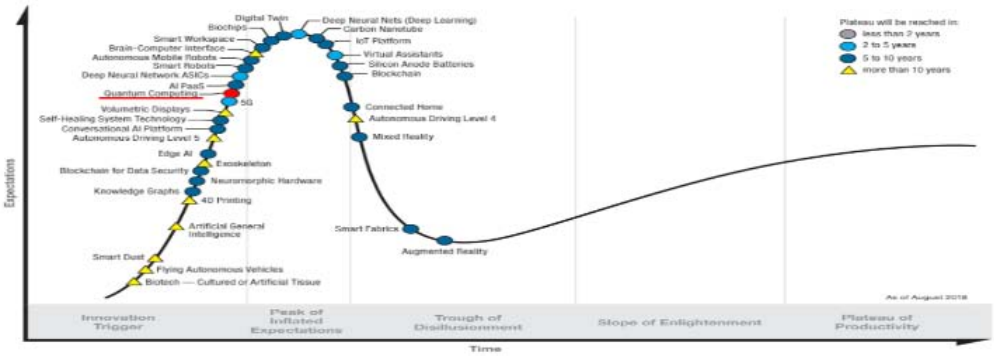


Figure 5. The arising technology in 2018 [27].

Furthermore, the Google search engine revealed that quantum computation is a hot topic on the internet (last five years) where the peak was in 2019, as seen in Figure (6).

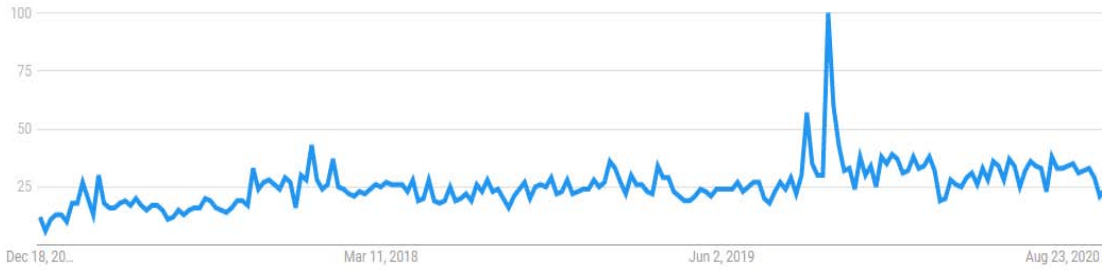


Figure 6. The trending of quantum computing [28].

1.4 Quantum bit

The bit is the basic unit of data, which expresses a two-valued number, when answering the question by yes or no this represented the two of values, the position of the flip when it is on or off, or a stop/go decision. Unbreakable bits are used to construct all computerized computing devices. Normally, the integrability and 1 signify a bit's worth [29]; A quantum bit (Qubit) can be 0 , 1 or in unknown state as the two states at the same time called superposition)[27]:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.2}$$

Where: $|\psi>$ the quantum bit state.

A and β : the amplitude, must meet one requirement:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{1.3}$$

then, the superposition state is:

$$\left(\frac{1}{\sqrt{2}}\right)^2 \alpha + \left(\frac{1}{\sqrt{2}}\right)^2 \beta = 1 \tag{1.4}$$

The rest of the states will be split from them. Quantization gave rise to the quantum concept, which implies that such quantities can only be given on a discrete set. In the

quantum universe, particles can only have those energies. Since particles are waves, they do not take on any form; but each shape has a corresponding energy, which is what quantification is. These levels of energy aid in the comprehension of atomic structure and the creation of new computing devices [31].

Because of the enormous role that the quantum bit plays in the quantum computing universe, it is important to think about it in detail. The criteria that are shared by quantum bit innovations are:

1. A two-stage physical structure for running as a qubit;
2. An implication for qubits initialization into a superposition;
3. Between them, there is an all-integrating series of gates;
4. The two stage can be measured.;
5. A long-term memory [30], more details in [31].

There are several kinds of Qubit, it relies on the purpose of the usage, but the following are the most common types[31]:

1. Photon as Quantum bits: also called an ion trap: it uses ion spin; for materials it uses atoms, recently, the maximum proved variables are 16 that can be used.
2. Quantum dot: it uses Electron spin, position, or energy level, the maximum proved variables are 3.
3. Optical circuit: it uses Photon polarization, position, or time, the maximum proved variables are 8.
4. Gate-based superconducting circuit: it uses a time, Magnetic flux, or current phase; the maximum proved variables are two.
5. Photon as Qubit: it uses the polarization photons to represented the quantum bit, it used two states, rectilinear polarizations of 0°, 90° and diagonal polarizations of 45° and 135°.

For the binary state "0", legitimate sender and receiver, denoted by Alice and Bob, settle on 0° or 90° to represent it, whereas 45 ° or 135 ° will represent the binary state "1".

1.5 The thesis motivation.

With the billions of devices deployed under the internet of things (IoT) paradigm, and the massive deployment of these devices under the 5G massive machine type communication (mMTC) use case, security challenges have risen, due to the limited battery energy and computational power of many of these devices [32], [33].

Furthermore, this deployment is expected to become more massive under sixth generation (6G) networks, with increased deployment of IoT devices related to mission critical services, thus expanding the 5G ultra-reliable low-latency communications (URLLC) use case into a massive URLLC (mURLLC) scenario in 6G [34].

The advancements in computations accompanying the 6G era, notably in the area of quantum communications, have exacerbated the security challenges related to IoT devices. In fact, these devices need to be protected from security breaches in the face of adversaries that potentially have quantum computing capabilities [35].

Therefore, we address the problem of using quantum cryptography to enhance the protection of these devices in the 6G era. Due to their limited power and computational capabilities, it would be unreasonable to assume that IoT devices can handle quantum communications by themselves. Here comes the role of IoT controllers, that are present in many IoT applications in order to collect, aggregate, and process data from multiple IoT sensors, before transferring this data over the network to be stored on remote servers for processing and analysis [36].

The controllers are generally more powerful devices and can securely communicate with the server using cryptographic techniques. In this paper, we use these controllers to perform quantum key distribution (QKD) and then distribute the generated keys to the IoT devices so that they can encrypt their data over the traditional radio frequency (RF) communication links between them and the controller. Thus, QKD is performed by the controllers to protect the weak IoT device - Controller link from malicious attackers.

1.6 The thesis contribution.

The contributions of this thesis can be summarized as follows:

- Using easy and functional code in this thesis to measure the length of a key for certain number of photons (quantum bit).
- Using BB84 QKD generation to describe the photon polarization states used for adopting optical fiber to relay high-security telecommunication information.
- Proposing a simple, convenient, and effective way to simulate a quantum key distribution.
- Generating and measuring the final key length for the specified number of initial photons (Qubit).
- Implementing an algorithm in real-life quantum computer.
- Generating a true random number (that generated in the previous point) to use in the proposed simulation. Using the final length key for symmetrical protection for IoT devices (lightweight).
- Simulating of the attacker between the server and IoT devices.
- Proposing and simulating a new way for detecting the attacker.

- Using machine learning to detect an attacker by relying on the final quantum key length, even though the effect of that attacker on the quantum key was within the acceptable threshold range.
- Evaluating the effect of Increasing the initial photons on the final key length by using the proposed simulation method.

1.7 The thesis organization.

This thesis is organized as follows: Chapter 2 discusses the quantum applications that have used quantum in general, and also justifies why this method of communication was used in applications such as quantum radar, quantum communication within a quantum computer, quantum satellites, and quantum sensing. Quantum key distribution is one of the quantum mechanics applications in terms of communication. It is used to protect the transmission between the sender (Alice) and receiver (Bob). As a result, chapter 3 addresses the proposed mechanism and general structure of using quantum encryption, as well as how it is used for protecting IoT devices. Subsequently, chapter 4 describes quantum key distribution as the protocol used to secure the messages. Besides, several simulators that have been used to simulate quantum key distribution are explained in this chapter, along with their benefits and drawbacks. The chapter also goes on to describe the proposed simulator and its benefits, as well as how to use a real-world quantum computer (IBM) to generate random numbers for the proposed simulator. In the end, the chapter shows the solution for quantum key distribution in the presence of an attacker. Chapter 5 investigates similar works, indicates and explains the simulator's effects, and depicts the simulation of an intruder between the sender and the receiver. Chapter 6 defines the machine learning algorithms that are used to detect an attacker within the approval

final key length (which does not surpass the threshold) and then explains the results; at the end the chapter shows the solution after detecting an attacker. Finally, chapter 7 summarizes all of the research findings and conclusions contained in this study, as well as potential studies that constitute interesting future research directions.

CHAPTER 2: QUANTUM COMMUNICATION APPLICATIONS

Future information communication technology (ICTs) will certainly focus on quantum communication technologies (QCTs) that are built over the laws of quantum physics to secure data communication, developing preparations for this emerging important future field. In upcoming ICT, not only do computers benefit from quantum technologies, but our contact will also move to quantum. Instead of the conventional Internet, the quantum Internet is used as a modern channel of contact. The latest research is now focused mainly on quantum internet and quantum teleportation, as it is now the most suitable technology.

The most applied Quantum Internet is a security application, which is used to secure communication between the sender and receiver as it is based on quantum mechanics' law. Quantum security guarantees the high privacy of future quantum Internet, where not only data can be shared securely, but also multiple quantum devices can be grouped in the cloud and share huge computational power. moreover, there are many other applications such as radar, satellite, etc.[37].

2.1 Quantum radar (QR)

In order to enhance the identification, the possibility of detection, and the discrimination of stealth platforms (planes, drones, etc.), it is essential and significant to improve a classic (current) radar, and so are improved sensors. The US has long been developing and using stealth technology, while China has also developed its stealth fighter. However, stealth technology is being more widely used in the military, as a series, it is essential and crucial to providing an early warning mechanism against stealth and other enemy attacks [38], earth discovery, a massive volume of man-made and natural waste circling the Planet from old spacecraft and small rockets, presents a

significant challenge to man-made and unmanned exploration of space [39]. Defending the universe, the comets, and the detection of asteroids, and other celestial bodies, that may be on the course of the earth and collide with it. In the last decade, however, there has been an interest in the mitigation techniques for planetary defense.

The QR has used the same principle as traditional radar, which transmits electromagnetic radiation, also, the antennas used by the quantum radar are the same such as dish antennas, or phased array antennas, or sometimes multiple-input multi-output (MIMO) antennas.

QR when used EM in the shape of photons holds a copy of the transmitted photons (e.g. when using two photons send one photon and holds the other one), but these two photons are entangled, this is different then what happens in the CR, the CR when transmitted waveform uses a mathematical representation to the matched filter. Because the two photons have an entanglement, this will give more much information between the two photons, which is used by the related filter. Two photons are assumed to be "entangled" if they cannot be described as two independent particles and must be regarded as one quantum mechanical being [40].

2.2 Quantum communication inside quantum computer

By exploiting quantum mechanics, the new computation paradigm produced the quantum computer to provide new ways for trying to solve problems that are currently thought to be difficult to solve. In the 1990s the algorithm of Shor was introduced for factorizing integer, in the same decade Grover's search algorithm was proposed. The last decade witnessed an impressively rapid growth of quantum technology, both from hardware implementation and hypothetical work perspectives. However, recently, the current quantum computers are not sufficient to

run good quantum processes, such as the Shor's algorithm needs for 1000 Qubits to run.

Recent achievements quantum computer such as what called a quantum supremacy has introduced the so-called noisy intermediate-scale quantum (NISQ) stage. Quantum computation has advanced at a quick speed, both theoretically and in terms of hardware execution, in the previous decade. However, existing quantum machines are partly efficient to run successful quantum algorithms at the state of the art of classical algorithms. The so-called noisy intermediate-scale quantum (NISQ) stage has been implemented as a result of recent accomplishments such as quantum supremacy.

NISQ devices have a variety of problems, including decoherence errors, noisy gates, and erratic readout measurements, restricting their efficiency. Quantum technologies, even at this early stage, can provide useful tools for a wide range of applications. On the one hand, NISQ processors are well adapted for certain typical completely determining algorithms, such as algorithms designed to address some problems in high energy physics (HEP).

The quantum communications inside the quantum computer rely on the quantum bit with the characteristics of the inside components such as the quantum CPU, quantum memory, make computation possible because the probability of the quantum bits led to errors and then need for error correction(it is a separate topic, we do not discuss it in this thesis). It manages the contents, and all these components have a mission, to control, monitor, and operate the Qubit [41], [42].

2.3 Satellite quantum communications.

Fiber optic offers point-to-point links because the optical attenuation of these links is limited to a few hundred kilometers, also, due to the curvature of the Earth and atmospheric attenuation and turbulence, there is a limitation for free-space links. On the other hand, the quantum repeater will extend such limits, moreover, the roadmaps of much continental information-and-communication technology fostered the free-space satellite links would make them possible by the quantum global communication network realization.

Indeed, entanglement swapping, the measurement of Bell inequalities in a relativistic scenario, as well as, quantum teleportation, need for quantum communication (QC) over long distances, in special, along with satellite links. Therefore, after the end of 2007, space-to-ground links have simulated experimental studies of single-photon level by exploiting laser-ranging satellites. However, polarization encoded quantum key distribution in space requires qubits prepared in different polarization states, which are the QC core [43], [44].

2.3 Quantum sensing.

When using quantum characteristics, quantum system, or quantum phenomena (collection of coherently interacting objects is transformative in the investigations) one of the definitions is "quantum sensing"[45]. Nowadays, the branch of research within the area of quantum science and technology that uses quantum sensing has grown distinctly and quickly. Moreover, it is used for ong -term and short-term experiments, also, it gives a set of platforms, it is used to measurement beyond the classical possibility by using quantum entanglement communications, one of the valuable applications is detecting dark matter [46].

CHAPTER 3: QUANTUM KEY DISTRIBUTION FRAMEWORK

Due to increased attack surface (many susceptible systems), increased attack number and complexity, uniformly linked computers, attack speed, and attack tool availability and simplicity, all these facts make hacking the number one crime to worry about, growing in security incidents in 2009 by 3.4 million to reach 42.4 in 2014.

Cryptography is the art of preventing unauthorized access to private records, maintaining the confidentiality and security of files, and other activities. Classical cryptographic technology in use today is based on the hardness of certain numerical methods, such as integer factoring or the problem of discrete logarithms. However, because these problems are usually not known to be challenging to a malicious entity with quantum computing capability, the resulting cryptosystems are theoretically insecure.

Code-based cryptosystems, such as the Diffie-Hellman key exchange and the Rivest-Shamir-Adleman (RSA) and ElGamal cryptosystems, are among the most promising encryptions that still rely on the hardness of the integer factorization or discrete logarithm problems [35].

Quantum computers are now the digital world's reality. It is a fact that as a new invention arrives, it acts as a solution to the current challenges, but also carries fresh security concerns as are the case for Quantum Computing. By quickly solving complex mathematical problems, these machines are able to crack the existing public key infrastructure, such that can be broken by Shor’s algorithm. Also, post-quantum cybersecurity is now one of the most widely studied areas of cryptology to modeling the age of the post quantum computer such that multivariate public key cryptosystem [47].

Moreover, significant advancement in communications technology, like the internet of things (IoT), has exceptionally transformed the sensing of surrounding environment. IoT Innovation enables modernization that enhances the value of life and is capable of collecting, quantifying, and understanding the environmental conditions.

This circumstance helps to simplify the new ways of communication between things and humans, therefore facilitates the generation of intelligent modern cities. Internet of things is also one of the fastest emerging areas from beginning of the computing fields with approximately fifty billion devices by the start the year 2021. IoT technology plays a critical part in improving actual life by providing smart technologies, such as intelligent universal health care, intelligent homes, intelligent transport, and intelligent education.

Conversely, the implementation of complex special security in the landscape of IoT devices has introduced systems difficulties. Keeping the security needs in a significant IoT threat environment is a challenge. Challenging internet of things security structures are attributable to limited computing, connectivity, and power consumption resources. Furthermore, independent IoT systems should continue to figure out how to survive in a comprehensive and consistent manner, with safe operation as the main concern, especially in situations under which threatening circumstances, like the healthcare services, may arise. New attack surfaces are now being presented in the IoT environment.

Such attack areas are triggered by interconnected and interdependent IoT systems. As a result, the protection against the threats are at greater danger in IoT applications than in other applications and services and the conventional solution may be inefficient for these kinds of technologies.

One of the most basic cryptographic primitives is the establishment of symmetric keys among two distant parties via an insecure network, and it underlies many cryptographic schemes that are used nowadays. Public-key encryption is widely used to achieve this. No other approach can be found which does not use outside of the band's communication, quantum communication, or third parties that are trustworthy.

Quantum key distribution (QKD) facilitates the key establishment via an untrusted network like classical public-key cryptography. This approach is known as the distribution of quantum keys, thus the naming QKD. The protection of QKD relies on the natural phenomena of quantum mechanics, not on the complexity of mathematical problems, and is able to be demonstrated even against an eavesdropper, an attacker, who has infinite computational capacity.

If the key is produced as long as the plain text (message) that is to be transmitted and is used once only one-time pad (OTP), the encrypted message (cipher text) cannot be returned to the plain text for any computing capacity, including the most efficient equipment. The theoretical security of information is known as this kind of security. Since the beginning of the BB84 protocol, and so the other quantum security protocols have also been developed and introduced such as E91 protocol, etc., for distribution of the key that was generated to ensure secrecy between two devices [48].

QKD produces a secret key of random photons (Qubit) in an end-to-end relation. A transmitter, a receiver, and two communicating networks compose QKD communication. One is a quantum channel connected to the transmission of quantum random-bit signals by the encoder side and the decoder side, another is a conventional channel linking the main distillers. For the filtration of the main, the primary distillers perform error correction and privacy clarification on exchanged random pieces.

An attacker, who has infinite computing capacity, is able to enter the quantum and

conventional networks, but cannot contact the encoder (polarization filter), decoder (polarization filter at the receiver side), and key distiller's internal bits , thus attacker (Eve) cannot detect the key.

It is important to authenticate the classical channel, called the public channel. By checking the changing in the threshold that is calculated before the transmission, the sender and the receiver will detect it as Eve snoops on the quantum medium in all ways approved by the rules of physical science. If the error goes above a certain threshold and leads to discarding random bits along those limitations, the sender and the receiver stop producing the secret key, in comparison to the BB84 and B92 protocols, the EPR Protocol also uses Bell's inequality to define the presence or lack of Eve as a secret feature. The quantum protocol of the EPR is a protocol of three states [49].

On the other hand, the public map of a multivariate public key cryptosystem (MPKCs) contains a set of quadratic polynomials over a finite field. The NP-hardness of the problem of solving nonlinear equations over a finite field is provided by its primary safety assumption. This area is called to be one of the big PKC groups that even the strong quantum computers of the future could theoretically avoid. In the last two decades, there has been rapid and intense growth in Multivariate Public Key Cryptography [50]. Some constructions are not as stable as was originally believed, but others are still viable.

A Key Encapsulation Mechanisms (KEM) enables a symmetric key to be encapsulated under any public key inside a ciphertext, such that the symmetric key can be decapsulated again (only when) the corresponding hidden key is identified [51]. Security-wise, indistinguishably from a random string, the ciphertext conceals the encapsulated symmetric key [51].

In addition, Quantum Key Distribution Differential Phase Shift is a protocol suitable for fiber transmission systems and provides higher efficiency of key output than traditional BB84-based fiber. A photon divided into three pulses is sent from Alice to Bob in this scheme, where the phase difference between two consecutive pulses carries bit data. Via passive differential phase detection, Bob tests the phase difference.

We propose a flexible framework for implementation with IoT devices, at the outset we propose a simulation and generation of QKD, to make it more realistic to implement a part of the algorithm in a real-life quantum computer. In addition we secure IoT devices by implementing the BB84 protocol with the proposed simulation, and perform simulation of the QKD with the attacker in the middle to calculate the effect of the attacker on the final quantum key length. Then we calculate the correlation between the initial photons (in the sender) with the final key length and affect the increase in the length of the initial photons, and set the data for the final key length in the presence and absence of the attacker.

Finally, we use Machine Learning to detect the attacker by relying on the final key length to increase the initial photons to avoid the attacker.

3.1 Simulating and generating the QKD.

The main advantage of the proposed method is that it is more practical than the other methods [52], [53](see part 4.2), as each number in the algorithm (a random number between 1 and 4) represents the polarization status of the photon, while the other methods simulate the final decision "0" or "1". The proposed method simplifies significantly the randomness of the generation of the quantum key, and the process will also estimate the number of each polarization state (such as how many 0°, 45°,

90°, and 135° photons can be used), so it is better to use a real random number generator that relies on physical effects in the algorithm.

In the proposed simulation, we produce a random number used in the equation using a real-life quantum computer to make it more realistic. It is totally unpredictable, as it's hard to understand the position of the quantum now or in the future, so it creates a condition that cannot be expected for the polarization photon. So that QKD makes it difficult for an attacker to speculate by using photon polarizations.

3.2 Implementing the QKD by BB84 protocol.

The first QKD protocol was suggested by Bennet and Brassard in 1984, referred to as BB84. Alice has to give Bob a private key, they will come up with a shared key that can then be used with a symmetrical encryption process, such as a single pad. Alice has four polarized filters, each stream has one of four separate polarizations. Both of the two polarizations represents "1" or "0" and can be exchanged with Bob. Photons are used as qubits in the initial formulation of the protocol and the information is retained in their polarization.

Today, BB84 is the most common and efficient quantum cryptography protocol that transmits data using photon polarization states. The QKD protocol typically consists of a quantum channel and an authenticated traditional public channel.

In quantum cryptography, as a universal convention, Alice passes quantum bits (states) to Bob through a quantum medium. The eavesdropper Eve has been accused of listening to the quantum channel.

3.3 QKD for securing IoT devices.

QKD provides a special way to exchange a random series of Qubits between

clients including a degree of anonymity that cannot be obtained by encoding data in quantum states with any other classical cryptography approach to transmit a random secret key.

In an mHealth scenario for example, IoT sensors mounted over the patient's body would transmit the data to the IoT controller, who would transfer the data to the access point (AP), e.g. by Wi-Fi, and from there via the internet to the relevant cloud service for retrieval, processing, and analysis by medical professionals.

An attacker with infinite computational power is able to penetrate the quantum and classical networks, but cannot reach the encoder (polarization filter) and the decoder (polarization filter on the receiver side) so that the attacker (Eve) cannot detect the key.

In this case, the quantum channel will be a free-space optics (FSO) transmission channel, for example, and the keys shared would be used to encrypt data transmitted over a standard radio frequency (RF) channel, e.g., Wi-Fi or 5G.

3.4 Using machine learning with QKD for detecting attacker.

The neural network architecture consists simply of three layers, an input layer where the data is obtained from the user, a hidden layer(s) that transforms the input data into an acceptable type using unique parameters (weights and bias) that can be used conveniently later in the output.

The network structure will be trained on the testing portion of the dataset and then checked on the test data and this process is replicated for many epochs and various parameters can be modified (as number of hidden neurons and number of hidden layers) until the least error is reached, in this case this model architecture will be chosen. The biggest benefit of using a neural network approach is that it is a data-

driven approach that can process data without any explicit constraints or back-knowledge assumptions regarding the model type.

We used MATLAB toolbox to implement our work. This toolbox includes algorithms, pre-trained models, and applications to develop, train, imagine, and simulate neural networks with either one hidden layer (called a shallow neural network) or multiple hidden layers of deep neural learning.

For our research, we used a shallow neural network to deal with a large dataset (about 20,000 samples). We do not need deep networks because we do not have a large number of features, and the dataset is not very complex.

CHAPTER 4: QUANTUM KEY DISTRIBUTION SIMULATION

Cryptography is the art of preventing unauthorized access to private records, maintaining the confidentiality and security of files, and other activities [54].

QKD facilitates the key establishment via an untrusted network like classical public key cryptography.

The protection of QKD relies on the natural phenomena of quantum mechanics, not on the complexity of mathematical problems. Since the start of the initial protocol, BB84 , and with other quantum security protocols have also been developed and introduced such as E91 protocol ,etc., for distribution of the key that was generated to ensure secrecy between two devices [55]. One is a quantum channel connected to the transmission of quantum random-bit signals by the encoder side and the decoder side, another is a conventional channel linking the main distillers. An attacker, who has infinite computing capacity, is able to enter the quantum and classical networks, but cannot access the encoder , decoder , and key distiller's internal bits , thus attacker cannot detect the key [56].

By checking the changing in the threshold that is calculated before the transmission, the sender and the receiver will detect it as Eve as an attacker snoops on the quantum medium [57].

4.1 Quantum key distribution

Quantum Key Distribution (QKD) is a technology that requires parties (Alice and Bob) to be involved to share a secret symmetric key. If an attacker (Eve) attempts to snatch the secret key in a QKD protocol, communicators may use applicable quantum laws to observe it (e.g. the well-known Heisenberg uncertainty theory) [58].

In quantum mechanics, QKD usually relies on the inability to analyze a

structure without disturbing it. She would definitely leave any signs that can be detected, as Eve needs to eavesdrop on Alice and Bob's quantum correspondence. The QKD protocol thus achieves security. On the other hand, the protocol randomly produces long keys if Eve is passive.

In addition, the protocol identifies the attack and terminates the generation of keys as Eve tampers with quantum networks. The likelihood that the protocol does not stop and an attacker copies the generated keys is so tiny for any attack on quantum networks [59].

4.2 BB84 protocol

In 1984 the first QKD protocol BB84 was proposed. At the moment, BB84 is quantum cryptography protocol, it is the most general and powerful that transmits data using photon polarization states [58].

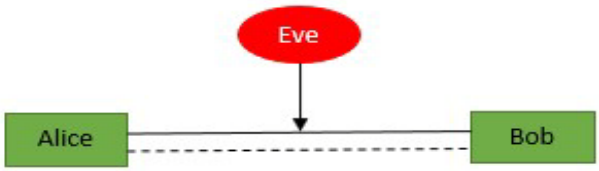


Figure 7. A QKD protocol generally consists a quantum channel (the strong line) and an authenticated classical public channel (the dashed).

In quantum cryptography, as a universal convention, Alice transfers quantum states through a quantum channel to Bob. An eavesdropper (Eve) is accused of listening to the quantum channel, as illustrated in Fig. 7. Alice and Bob can come up with a shared key that they can then use with a symmetrical encryption method, such as a one-time pad. Alice has four polarized filters, with each stream having one of four

different polarizations, each two of polarizations represent "1" or "0", and can be shared with Bob. Photons are used as qubits in the initial formulation of the protocol, the information being stored in their polarization [60] (see Fig. 7).

Alice wants to give Bob a private key. She starts with two sequences of bits, x and y, each of a length of n bits. As a tensor product of m qubits, she then encodes these two strings [61]:

$$|\psi\rangle = \bigotimes_{i=1}^{m} |\psi_{x_i y_i}\rangle, \tag{4.1}$$

Where x_i and y_i respectively are the i-th bits of x and y. Together, $x_i y_i$ gives us an index in the four qubit states below:

$$|\psi_{00}\rangle = |0\rangle \tag{4.2}$$

$$|\psi_{10}\rangle = |1\rangle \tag{4.3}$$

$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{4.4}$$

$$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \tag{4.5}$$

Equations (4.4 and 4.5) represent the superposition state, and we can get them by applying Hadamard gate (for more details see Section 4.3.3).

4.2.1 Simulating models according to System Dynamics methodology (OptSim).

For device simulation, RSoft, OptSimTM program from Synopsys Inc is used. Using a time domain split-step algorithm, the program solves the nonlinear Schrodinger equation. The program includes templates for various optical instruments and the analyzing methods [62].

The incoming light of photons in OptSim PBS is divided to horizontal or

vertical distinct angles. Some of the elements present in the OptSim collection are not executed as elements of QKD. A modification or formation of components is necessary in these situations.

OptSim has several more constructed libraries called visualizers that could be used for simulation. In this library, elements of the polarity analyzing and powering meter for photon detection and counting can be manipulated. In the communication network, there are three important classifications; they are, channel, source, and destination [63].

4.2.2 QKD simulation using python QuTiP.

QuTiP offers an object-oriented architecture to represent and execute calculations and simulations of generic quantum systems on those systems. One must first create an entity that encapsulates the properties of an arbitrary state vector or operator in order to simulate a quantum system.

Using the quantum object class (Qobj), which uses a sparse matrix representation of a quantum object in a finite dimensional Hilbert space, a coherent representation of quantum operators and state vectors is performed in QuTiP.

Internally, the Qobj class holds a list of the key properties of the quantum object that its represents. These include the type of entity (i.e., Bra-ket notation , operator, or super-operator), if the underlying object is Hermitian, the dimensionality of the composite object generated by the product tensor, and the size of the matrix of sparse details [64].

Using Python packages such as QuTiP, QKD is introduced using the BB84 protocol and makes use of different scientific libraries. The software was designed in such a way that, as in the actual quantum system, it can replicate the quantum world

and maintain the randomness of the system. Figure (8) illustrates the way of the implementation for BB84 protocol [52].

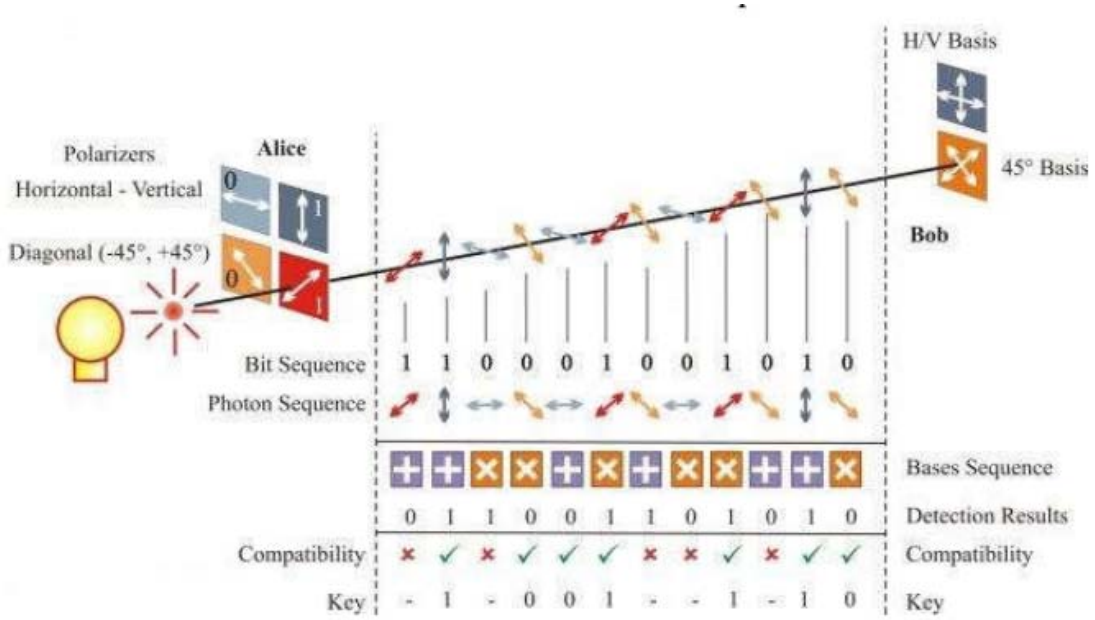


Figure 8. Working demonstration of BB84 protocol.

4.2.3 Modeling Fuzzy Logic in Simulink to simulating QKD.

Dr. R S Kumar of the Department of Computer Engineering Defense Institute of Advanced Technology (DIAT) proposed a new Modeling Fuzzy Logic at MATLAB Expo, Pune, India, in 28 April 2015 [65].

Using Simulink, Quantum Key Distribution, in MATLAB, the Fuzzy Logic toolbox includes a fuzzy controller block which can be used to model and simulate a fuzzy logic control system in Simulink. The Toolbox offers: FIS Editor, Membership Function Editor, Rule Editor, Rule viewer and Surface viewer, (see Figure 9).

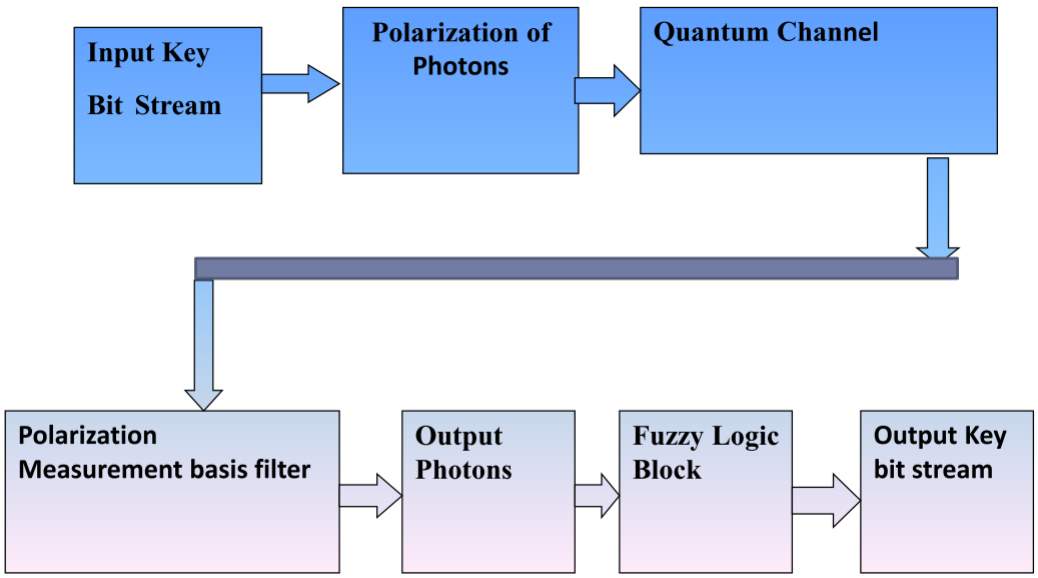


Figure 9. Fuzzy Logic QKD [65].

4.2.4 The Proposed method for generating and simulating QKD

To build photon streams, Alice has four polarized filters where each stream has one of four distinct polarizations, rectilinear polarizations of 0 °, 90 ° and diagonal polarizations of 45 ° and 135 °.

For the binary state "0", Alice and Bob settle on 0 ° or 90° to represent it, whereas 45° or 135° will represent the binary state "1", as shown in Table 1.

Table 1. The polarization states and corresponding bit represented.

Polarization/bit	0	1
Rectilinear +	↕	↔
Diagonal x	⤢	⤡

Alice produces the first step of the main source. Alice generates a polarized photon stream, choosing their polarization at random. Alice transmits these photons one polarization at a time through the quantum tube. Alice makes a note of the unpredictability polarization chain that Bob has no way of guessing what polarization

any of the photons has.

Bob has two detectors:

- A rectilinear filter (+): Photons with a rectilinear position move unchanged into this filter, the rectilinear filter switches to a random rectilinear state (0 ° or 90 °) the state of a diagonally polarized photon.
- Photons with a diagonal state pass unchanged across a diagonal filter (x). The diagonal filter alters the state to a random diagonal state (45° or 135°) of a rectilinearly polarized photon, as described in Table 1.

When each photon arrives, Bob arbitrarily guides it to one of his two detectors, then Alice and Bob interact over the normal contact channel to address Bob's detector preference, discarding all the wrong bits that Bob acquired from an incorrect filter range. To extract a shared key stream, the remaining bits are then used. Eve follows the same approach used by Bob, sometimes using the right detector and sometimes the wrong detector. If her decision is correct, the photon will continue with its prior polarization on its path.

If her decision is false, she is going to change the polarization of the photon that she passes on to Bob. The resulting bit stream would not be right in any way due to Eve's interference at the end of Bob's detection, and after consulting with Alice to discard wrongly observed photons, Alice and Bob execute a single search before the mutual key stream is used comfortably. If they discover a bunch of mismatches, they publicly pick and compare several bits picked at random from their key streams, and if the error rate crosses a negotiated threshold, they delete the whole key stream and produce a new one.

In Table 2, we took 50 cases from 500 photons up to 990 photons from the online simulator (the other simulator)[66]. Table 2 indicates that the number of initial

photons is 500 and the final key length is 129, both arrive and fit the polarization filter of the receiver. The length of the key is random, but when Alice sends the next time, the final key length will be different. The final key lengths for all corresponding initial photons do not follow the same pattern as the initial photon, but instead, increase and decrease at random. Also, we took the number of sent photons (Qubits) and the final key length and analyzed them by using SPSS to find the correlation for the online simulator.

Moreover, as part of our work, we simulate 7010 up to 7500 photons (Qubit) (see Figure 10, Tables 3, 4, and 5). We used these numbers of photons to show that our approach is flexible and can be used with any photons, moreover, we can compare our work easily with other scenarios such as in [67], where the authors have used (IDQ-Clavis2) device to generate and implement a QKD.

The main benefit of the proposed method is more realistic than the other methods since each number in the algorithm (the random number between 1 to 4) represents the polarization state of the photon.

The other methods simulate the final decision "0" or "1", whereas the proposed method actually indicates the randomness of the generation of the quantum key, and the method can also predict the number of each polarization state (such as how many photons with 0, 45, 90, and 135 can be used for other applications in pure physics science), therefore, in the algorithm it is preferable to use the true random number generator that depends on the physical phenomena.

Table 2. Initial quantum bit (photons) to Final key length for online simulator.

` Initial quantum bit (photons)	Final key length
500	129
510	144
520	148
530	127
540	146
550	162
560	147
570	162
580	180
590	168
600	153
610	173
620	184
630	199
640	193
650	185
660	206
670	186
680	210
690	208
700	203
710	204
720	228
730	227
740	207
750	227
760	212
770	252
780	252
790	272
800	258
810	252
820	266
830	267
840	257
850	268
860	284
870	272
880	303
890	287
900	283
910	298
920	321
930	295
940	299
950	292
960	296
970	324
980	333
990	332

Moreover, the plot of the initial quantum bit to the final key length illustrated in Figure 10.

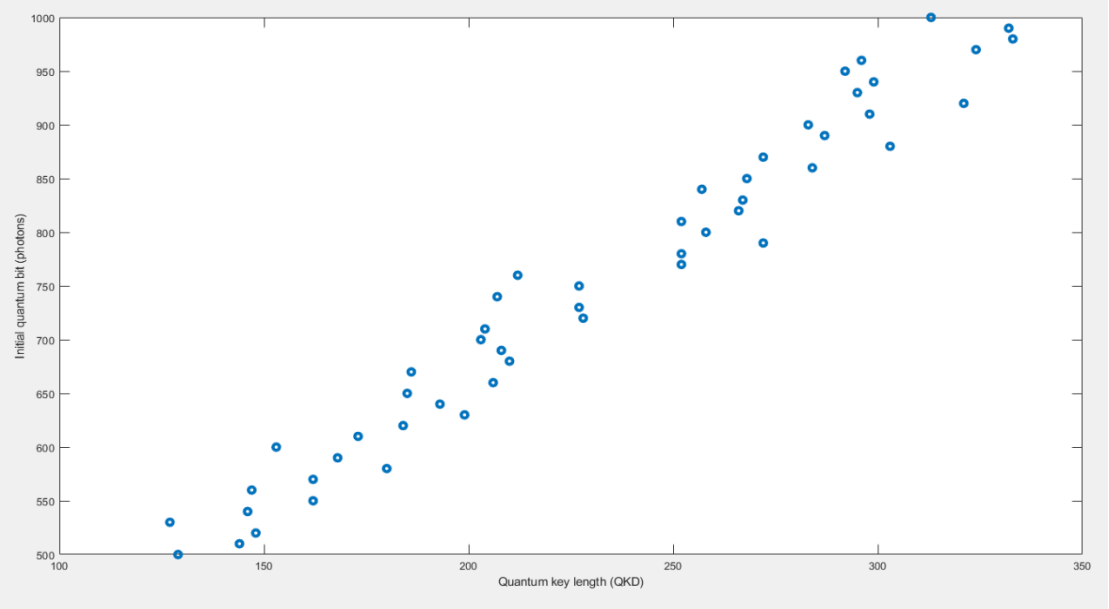


Figure 10. Initial quantum bit to the final key length for the online simulator.

In addition, we analyzed initial quantum bit to the final key length for the online simulator by using SPSS to find the correlation (see Table 3).

Table 3. The coloration between the initial quantum bit with the final key length for the online simulator.

		Initial number of qubits	Final key length
Initial number of qubits	Pearson Correlation	1	.983**
	Sig. (2-tailed)		.000
	N	50	50
Final key length	Pearson Correlation	.983**	1
	Sig. (2-tailed)	.000	
	N	50	50

**. Correlation is significant at the 0.01 level (2-tailed).

Algorithm 1: Algorithm for simulating and generating QKD.

```
1: A[i]=0;//declaration an array for the sender.
2: B[j]=0;//declaration an array for the receiver.
3: key[k]=0;
4: for i:=N;//N=number of photons (Qubits).
5: for m:=long number;//for increasing the randomness.
6: A[i]=rand(1,4)//prefer to be true random number that depend on natural phenomena such as noise of semiconductor, see section (4.3), we used real-life quantum computer.
7: for j:=N;//N=number of photons (Qubits).
8: for l:=long number;//for increasing the randomness.
9: B[j]=rand(1,4)//prefer to be true random number that depend on natural phenomena such as noise of semiconductor.
10: for m:=N;
11: if A[m]==B[m] then
12: key[m]=A[m];//key length;
13: if key[m]==1 then//For polarization 0 degree.
14: cont_pol_0=cont_pol_0+1;
15: if key[m]==2 then//For polarization 45 degree.
16: cont_pol_45=cont_pol_45+1;
17: if key[m]==3 then//For polarization 90 degree.
18: cont_pol_90=cont_pol_90+1;
19: if key[m]==4 then//For polarization 135 degree.
20: cont_pol_135=cont_pol_135+1;
```

Algorithm 1 describes the approach to generating the shared quantum key between Alice and Bob, which could be the server and each IoT device, respectively. At the beginning, we declare arrays for containing the random numbers for sender and receiver, also the last array is called key for containing the key values that were generated and reached the receiver. Line 6 generates a random number from 1 up to 4, each number representing a polarization of photon (Qubit) such as 1 for 0°, 2 for 45°, 3 for 90°, and 4 for 135°.

Line 11 compares the two arrays (representing the polarization of the sender and receiver photons), takes each cell in the Alice array, and compares with each cell in the Bob array (corresponding cell, such as cell A[1] compared to B[1], and so on). It guarantees that the polarization at each end is equal when the polarization is the same, then the polarization of the photon will be stored in the corresponding cell of the key array (e.g. when A[1] equals B[1] then A[1] stored in the key[1]), the loop will continue until the end of the arrays. This algorithm is dynamic as it can adjust the number of the sent photons to be equal to the number required for achieving the requested key length. The part from Line 13 to the end of the algorithm is dedicated to comparing and calculating the number of polarizations for each of the polarization that used 0°, 45°, 90°, and 135°. Table 4 indicates that the initial photon is 7010 and the final key for it is 2089 for the proposed simulator (thesis contribution). Both arrive and fit the polarization filter of the receiver. The length of the key is random, but when Alice sends the next time, the final key length will be different. The final key lengths for all corresponding initial photons do not follow the same pattern as the initial photon, but instead, increase and decrease at random, such as in the last number of initial photons is 7500 and the final key length is 2233, and when the number of the initial photon is 7490 the corresponding final key length is 2251.

Table 4. Initial quantum bits to final key lenth for the proposed method (thesis contribution).

Initial quantum bit (photons)	Final key length
7010	2089
7020	2108
7030	2094
7040	2093
7050	2121
7060	2104
7070	2110
7080	2113
7090	2117
7100	2109
7110	2139
7120	2122
7130	2125
7140	2140
7150	2130
7160	2147
7170	2138
7180	2152
7190	2157
7200	2154
7210	2166
7220	2168
7230	2157
7240	2178
7250	2174
7260	2167
7270	2188
7280	2172
7290	2167
7300	2190
7310	2178
7320	2181
7330	2179
7340	2197
7350	2183
7360	2202
7380	2212
7390	2222
7400	2219
7410	2215
7420	2230
7430	2217
7440	2231
7450	2242
7460	2226
7470	2243
7480	2246
7490	2251
7500	2233

Table 5. The coloration between the initial quantum bit with the final key length for proposed method (thesis contribution).

		Initial number of qubits for 7010 to 7500	Final key length
Initial number of qubits	Pearson Correlation	1	.983**
	Sig. (2-tailed)		.000
	N	50	50
Final key length	Pearson Correlation	.983**	1
	Sig. (2-tailed)	.000	
	N	50	50

**. Correlation is significant at the 0.01 level (2-tailed).

When the correlation between the initial photon and the final key length is equal, Table 5 of the proposed method (in this thesis) shows the same pattern as table 3 of another simulator (online).

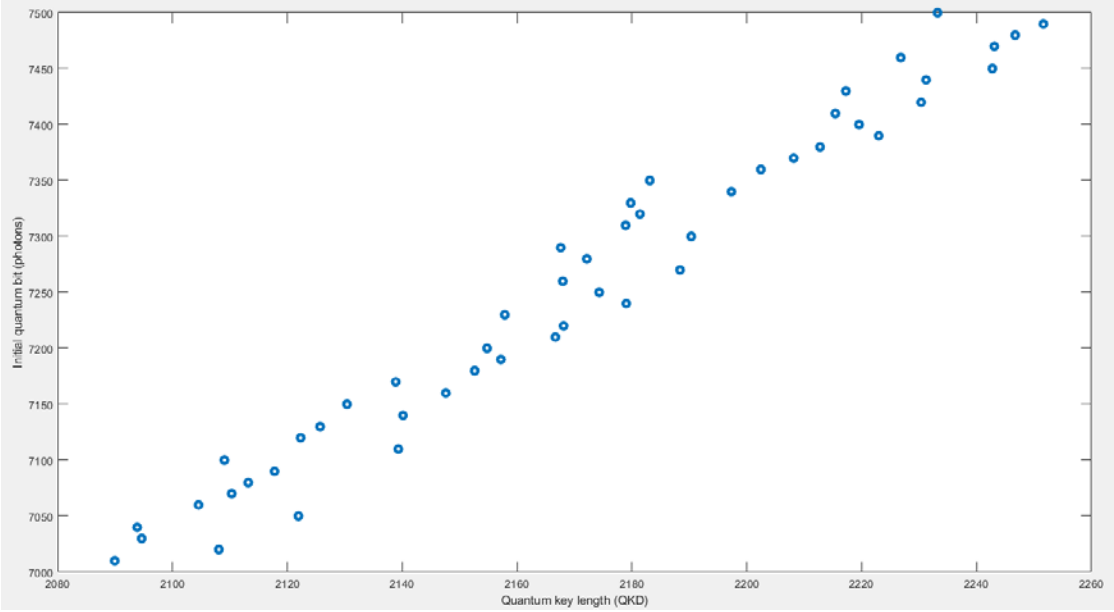


Figure 11. initial quantum bit to the final key length for the proposed simulator.

4.3 Generating random number by using real-life quantum computer.

Quantum mechanics is a natural phenomenon within the materials for tiny items, so it does not depend on any mathematical equations and we can measure or calculate

it and then give a predicated formula to know the velocity or location and then the state of the quantum bit would be simple to know. It is completely random, so it is unpredictable, it is difficult to understand the state of the quantum now or in the future, so it produces a state that cannot be predicted for the polarization photon, such that QKD makes it impossible for the attacker to guess while using the photon polarizations.

In our simulation, we generate the random number that is used in Algorithm (1) using a real-life quantum computer to make it more practical. We used online real-life quantum computer (IBM Quantum Experience)[68], there are three ways to use the quantum computer.

The most important thing in the quantum computer to execute a code, is that we should design an algorithm and then build a circuit suitable for the algorithm then implement it in a quantum computer.

4.3.1 Qiskit.

Qiskit [kiss-kit] is an open-source Software development kit (SDK), SDK is a set of tools for third-party developers to use in producing applications using a particular framework or platform. Qiskit is used for working with quantum computers at the level of pulses, circuits and application modules. By providing the full collection of tools required for communicating with quantum systems and simulators, Qiskit accelerates the creation of quantum applications.

There are two choices when trying to get started with Qiskit. Qiskit can be started locally, which is much more stable and private, or it can be started with IBM Quantum Lab's hosted Jupyter notebooks [68]. Qiskit has four main components:

- Terra: The base on which the remainder of Qiskit lies is Terra, the 'earth'

portion. It offers the basis for writing quantum packages at the point of circuits and pulses, improving them for various system constraints, and handling the collections of implementation experiments on remote-access computers. It defines the layouts for a desirable end-user interface, and also the proper management of optimization layers, pulse preparation, and communication with the backend, Qiskit Terra is divided into different key modules.

- Aer: The 'air' component, Aer, permeates all Qiskit components. Better simulators, emulators and debuggers are needed to really accelerate the development of quantum computers. By showing to what degree, they can imitate quantum computation, it lets the users to comprehend the traditional computation power. In addition, we can use Aer to check the proper functioning of recent and near-upcoming quantum computers. By expanding the boundaries of simulation and simulating the noise of the effects of realistic computation, this can be achieved. Using the Qiskit software stack, Aer offers a high-performance simulator platform for quantum circuits. It requires optimized backends of the C++ simulator to execute circuits compiled in Terra. It also provides instruments for the development of highly configurable noise models for practical noisy simulations of errors that occur on actual devices during execution. Three high-performance simulator backends are used in Aer.
- Ignis: The 'fire' aspect is devoted to combating noise and mistakes and finding a new course. In the presence of noise, this means better characterization of defects, improving gates, and computing. Ignis is intended for those who want to design codes for the correction of quantum errors, or who want to explore ways of characterizing errors using techniques such as tomography or even

find a better way to use gates by investigating dynamic decoupling and optimal control. Provided a minimal set of user input parameters, it provides code for users to easily create circuits for unique experiments. Three simple building blocks include the Ignis code.

- Aqua: The 'water' aspect is the life element. We must find real-world applications to make quantum computing live up to its standards. Aqua is where quantum computer algorithms are designed. It is possible to use these algorithms to construct quantum computing applications. Aqua is open to chemical, optimization, finance, and AI domain experts who want to explore the advantages of using quantum computers as accelerators for particular computational tasks. In various domains, such as chemistry, artificial intelligence (AI), optimization and finance, problems that could benefit from the power of quantum computing have been described. However, quantum computing requires very advanced abilities to meet the needs of the large population of practitioners at different levels of the software stack who want to use and contribute to quantum computing.

4.3.2 QASM.

QASM emerged as a language for formally describing a quantum circuit to render images for visualization purposes. As quantum computation progressed, the language was adopted as a way to specify quantum circuits as input to a quantum computer.

A QASM software defines the traditional bits and qubits, defines the functions (gates) on those qubits and the calculations required to obtain the traditional result by evaluating the qubits. Many variants of QASM have seen the light since its emergence

as a mark-up language for generating images. Quantum Inspire uses cQASM 1.0 [68].

4.3.3 The methodology used to generate random number.

The IBM Quantum Experience has limitations for the number of Qubits used by the user. Also, many users access it online to implement the program; therefore, there is a queue for the execution of any written programs.

Algorithm (2) is used to generate the random number and is executed by using the real-life quantum computer. For the algorithm, two quantum bits are used to generate four numbers will represent 1, 2, 3, and 4 that are used in Algorithm (1). A qubit is placed into the state by the circuit:

$$|\psi\rangle = \frac{(|0\rangle + i|1\rangle)}{\sqrt{2}}. \tag{4.6}$$

The measurement probabilities are:

$$P_0 = |\langle 0 \mid \psi\rangle|^2 = |1/\sqrt{2}|^2 = 1/2 = 50\% \tag{4.7}$$

$$P_1 = |\langle 1 \mid \psi\rangle|^2 = |i/\sqrt{2}|^2 = 1/2 = 50\% \tag{4.8}$$

See equations (2- 4) in part (1.4) for more information and complete comprehension. After executing the output will be different than expected see Table(6). The radius of the black ring indicates the decreased purity of the qubit state in the N-qubit state for qubit j, state $|\psi\rangle$ is given by:

$$\mathrm{Tr}\left[\mathrm{Tr}_{i\in[0,N-1],i\neq j}\ |\psi\rangle\langle\psi|\right]^2 \tag{4.9}$$

For a single qubit, the decreased purity is within the range [0.5, 1]; the value of one means that the qubit is not intertwined with any other entity. A decreased purity of 0.5 suggests, on the other hand, that the qubit is left in a fully mixed state and has some degree of entanglement over the remaining qubits of N-1, and probably even the environment. The phases of the amplitudes are 0 and $\frac{\pi}{2}$ for |0> and |1> , respectively, see Figure(12).

Figure 12: The color wheel correlates the angle of phase to color.

Algorithm 2: Algorithm for gerarating a true random numbers.

```
1: for i:=n;// where n the number of random numbers.
2:    qreg q[2];// declare two registers to generate the quantum bits.
3:    creg c[2];// declarer two registers to store the state of the quantum bits.
4:    h q[0];// declare a Hamdard gate.
5:    h q[1];
6:   cx q[0],q[1];// declare a not gate.
7:    measure q[0] -> c[0];// command to get the result for the state of the Qubit.
8:    h q[0];
9:    measure q[1] -> c[1];
1o:   h q[1];
```

In line 1, we assume there is no queue for waiting (i.e., the other users finished their algorithm or code to execute it). In line 4, declare Hamdard gate to make superposition between the two Qubits.

Four Hadamard gates, CNOT gate, and two measurements linked to performance are shown in Figure (13) to calculate the final state of the two quantum bits.

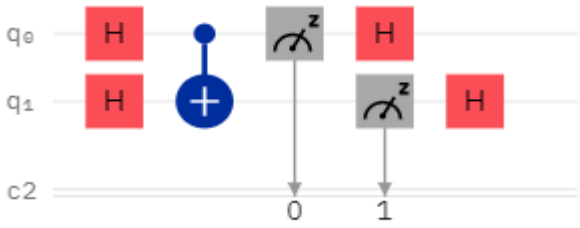


Figure 13: Original circuit for the algorithm to generate true random numbers.

Where: H gate: It is a single-qubit operation that assigns the base state |0> to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and |1> to $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, consequently, an equivalent superposition of the two base states is formed.

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{4.10}$$

CNOT gate: The gate is a two-qubit operation, where the first qubit is generally referred to as the qubit control and the second qubit as the qubit target.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{4.11}$$

Figure (14) illustrates the transpired circuit for the executed algorithm.

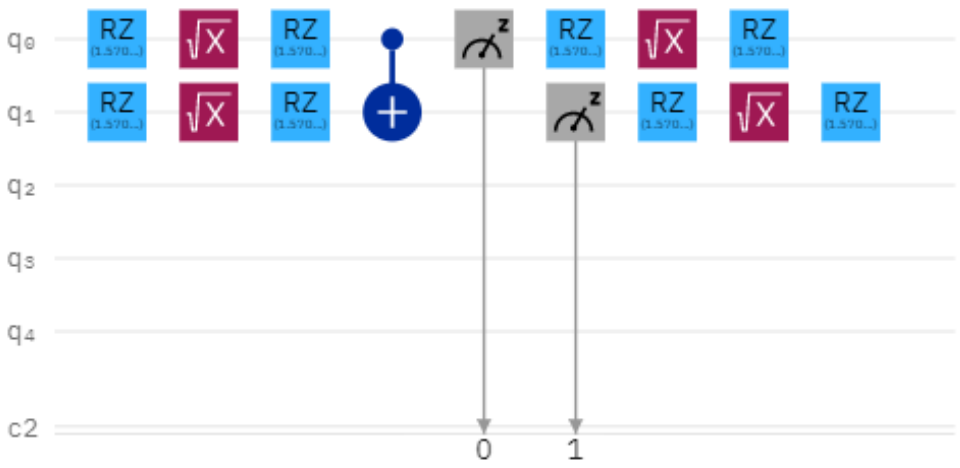


Figure 14: transpired circuit.

Where: RZ gate: It is one of the controllers of the Rotation. A single-qubit rotation via angle θ (radians) around the z -axis.

$$R_z(\theta) = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix} \tag{4.12}$$

For the 12 times, we implement the algorithm, we have the probability in the table of the results or the quantum states in Table (6).

Table 6: The quantum bits state.

Number of the execute	00	01	10	11	The represented number	The corresponding bit.
1	25.09%	23.53%	25.58%	25.87%	4, for algorithm 1.	1
2	28.9%	21.68%	23.53%	25.87%	1	0
3	29.29%	20.60%	23.14%	26.953%	1	0
4	25.19%	23.92%	25.09%	25.78%	4	1
5	25.39%	24.41%	26.07%	24.12%	3	0
6	25.78%	22.75%	23.92%	27.53%	4	1
7	23.633%	25.19%	24.6%	26.56%	4	1
8	24.31%	25.39%	23.82%	26.46%	4	1
9	25.29%	24.7%	23.43%	26.56%	4	1
10	25.78%	23.14%	23.82%	27.24%	4	1
11	23.04%	25.97%	25.48%	25.48%	2	1
12	26.85%	26.07%	22.07%	25%	1	0

After implementing Algorithms (1) and (2), we got almost the same results that was shown in Section (4.2.4). For more details see Table (7).

Table 6 describes the random number used in algorithm 1 and generated by using a real-world quantum computer. It indicates the probability of the number because the quantum bit in the quantum computer works such that there's no certainty to measure the quantum bit. We take the highest probability of Qubit such as in the first one the bit "1 1" (the classical one) that represent number 4 is 25.87% of the probability of all the other bits, then we take these numbers and use them in Algorithm 1. We took only 12 cases for verification purposes, because there is a long queue for using online the IBM quantum computer. The number of generated of bits (0 and 1) is almost the same number ratio as in Table 4 and Table 7 that were generated by using MATLAB.

Table 7: The classical random number for 12 cases.

Number of the execute	The result number	The corresponding bits.
1	4	1
2	3	0
3	2	1
4	4	1
5	1	0
6	4	1
7	4	1
8	4	1
9	3	0
10	3	0
11	4	1
12	1	0

4.4 The novelty of the proposed algorithm for simulation QKD.

The proposed algorithm generates a random number and simulates the final key length, and man in the middle for the controllers, by generating random number 1 up to 4, each number representing a polarization of photons (Qubit) such as 1 for 0°, 2 for 45°, 3 for 90°, and 4 for 135°.

The main benefit of the proposed method is more realistic than the other methods since each number in the algorithm (the random number between 1 to 4) represents the polarization state of the photon, whereas the other methods simulate the final decision "0" or "1". The proposed method indicates the randomness of the generation of the quantum key, and the method can also predict the number of each polarization state. Also, the proposed, simulator shows how many photons with 0, 45, 90, and 135 degrees can be used for other applications in pure physics science. In addition, there is a limitation for other methods, that can generate QKD for a few initial photons, such as the one that we evaluate our work with[64], [66] can simulate the initial photon from 500 up to 1000, which is not practical because when it used with a massive number of IoT devices. furthermore, the proposed algorithm is $O(n^2)$ in term of time complexity make it faster than the other, and it has a few line less than 16, in other

hand, the others such as that implemented in python exceed 40 lines Finally, part of the algorithm generated by using real-world quantum computers to make the proposed method more realistic and novel than the other simulators.

CHAPTER 5: QUANTUM KEY DISTRIBUTION TO SECURE IOT DEVICES.

Significant advancement in communications technology, like the internet of things (IoT), has exceptionally transformed the perception of the surrounding environment. IoT Innovation enables modernization that enhances the value of life and is capable of collecting, quantifying, and understanding the environmental conditions [32]. This circumstance helps to simplify the new ways of communication between things and humans, therefore facilitates the generation of intelligent modern cities [69].

Internet of things is also one of the fastest emerging areas of the computing fields with approximately fifty billion devices by the start the year 2021 [70], [71]. IoT technology plays a critical part in improving actual life through smart technologies, such as intelligent universal health care, intelligent homes, intelligent transport, and intelligent education [33].

Conversely, implementing large complex security mechanisms in IoT devices faces difficulties due to the limitations of these devices in terms of power consumption and processing power. Achieving security in IoT with a significant threat environment is a challenge [72].

Classical cryptographic technology in use today is based on the hardness of certain numerical methods, such as integer factoring or the problem of discrete logarithms. However, because these problems are usually not known to be challenging to a malicious entity with quantum computing capability, the resulting cryptosystems are theoretically insecure.

One of the most basic cryptographic primitives is the establishment of symmetric keys among two distant parties via an insecure network, and it underlies many cryptographic schemes that are used nowadays. Public-key encryption is widely used

to achieve this. No other approach can be found which does not use out-of-band communication, quantum communication, or third parties that are trustworthy [73].

(QKD) facilitates the key establishment via an untrusted network like classical public-key cryptography. QKD produces a secret key of random photons (Qubit) in an end-to-end relation. A transmitter, a receiver, and two communicating networks compose QKD communication. One is a quantum channel connected to the transmission of quantum random-bit signals by the encoder side and the decoder side, another is a conventional channel.

An attacker, who has infinite computing capacity, is able to enter the quantum and classical networks, but cannot access the encoder (polarization filter), and decoder (polarization filter at the receiver side) [56], thus attacker (Eve) cannot detect the key. It is important to authenticate the classical channel, called the public channel. By checking the change in the threshold that is calculated before the transmission, the sender and the receiver will detect if Eve eavesdrops on the quantum channel. If the error goes above a certain threshold and leads to discarding random bits along those limitations, the sender and the receiver stop producing the secret key [55].

QKD offers a special way of exchanging a random sequence of bits between users with a degree of anonymity that cannot be accomplished by encoding the data in quantum states with any other classical cryptography method for sharing a random secret key.

5.1 Related work

By utilizing the states (four polarizations) of the photons describing the quantum key shared in the quantum link, the BB84 protocol [61] was implemented in [53]. In QKD experiments, to deliver the photons to the recipient, random polarization choices

are made. For the incoming photon measurement, the receiver often selects random polarization. Lastly, on the basis of polarization, detectors may be triggered. The public channel discusses all photon values reported by the sender and the receiver, which illustrates the fundamental function of the QKD situation.

Moreover, QKD is implemented using Python packages such as QuTiP in [52], where the authors have used BB84 protocol and the package makes use of different science libraries. The software was designed in such a way that, as in the actual quantum system, it can replicate the quantum world and maintain the randomness of the system. Furthermore, modelling Fuzzy Logic Quantum Key Distribution using Simulink is simulated in [65].

The architecture of the QKD network simulation module, which was built in the version 3(NS-3) network simulator, was shown in 2017 [74], the module allows QKD network simulation in an overlay mode or in a single TCP/IP mode.

5.2. Proposed methods

When each photon arrives, Bob arbitrarily guides it to one of his two detectors that Alice and Bob interact over the normal contact channel to address Bob's detector preference, discarding all the wrong bits that Bob acquired from an incorrect filter range.

To extract a shared key stream, the remaining bits are then used. Eve follows the same approach used by Bob, sometimes using the right detector and sometimes the wrong detector. If her decision is correct, the photon will continue with its prior polarization on its path.

If her decision is false, she is going to change the polarization of the photon that she passes on to Bob. The resulting bit stream would not be right in any way due to

Eve's interference at the end of Bob's detection, and after consulting with Alice to discard wrongly observed photons, Alice and Bob execute a single search before the mutual key stream is used comfortably. If they discover a bunch of mismatches, they publicly pick and compare several bits picked at random from their key streams, and if the error rate crosses a negotiated threshold, they delete the whole key stream and produce a new one.

Figure (15) shows the main configuration between the server and the IoT devices, we presume there are three IoT devices that exchange information with the server. We used a 3000-cell array of the first 1000 photons of these arrays used as the initial quantum bits to be sent to receiver number 1 (the first IoT device) to produce the secret quantum key bit, and so on for the other devices.

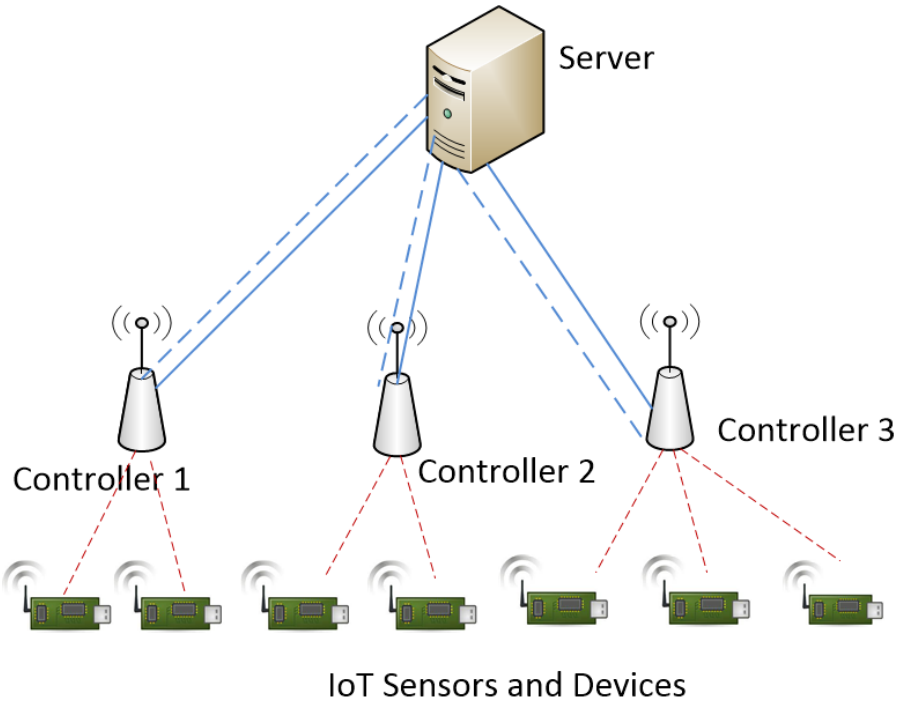


Figure 15: The structure of controller, IoT devices, base station and sharing the quantum key.

A practical use case scenario corresponding to Fig. 15 is the use of IoT devices in

mobile health (mHealth) scenarios. IoT sensors placed over a patient's body send measurement data would send the data to an IoT controller (corresponds to controllers 1-3 in Figure 15, and could be a smartphone for example), which would relay this data to an access point (AP), e.g., using Wi-Fi, and from there through the internet to an appropriate server on the cloud for storage, processing, and analysis by medical personnel [75], [76]. Naturally, security and privacy of patient's data is of utmost importance [36]. Thus, using QKD between the AP and controller would ensure strong protection against potential eavesdroppers. In that case, the quantum channel would be a free space optics (FSO) communication channel for example, and the keys exchanged would be used to encrypt the data transmitted over a regular radiofrequency (RF) channel, e.g., Wi-Fi or 5G.

Another use case scenario for QKD for IoT is the railroad monitoring scenario. Various IoT sensors can be used to monitor track parameters in real time (temperature, tilt, dip, shock, and vibration measurement for example), and send their data to an IoT controller (corresponding to one of controllers 1-3 in Figure 15). The controller would then send this data to a control center where the parameters are monitored in real time to ensure safety and security of the rail track. In such a case, fiber optic cables could generally be deployed along the rail tracks to provide backbone internet connectivity for remote areas. Thus, QKD can occur over fiber optic cable between the remote server and the IoT controller, and the keys exchanged can be used to encrypt the data between the controller and the various IoT sensors monitoring the track, over a suitable RF channel, e.g., millimeter wave 5G communications or Zigbee.

5.2.1 The method for quantum key distribution (QKD).

This section describes the approach for QKD. The objective is to securely distribute a secure key that can be used with symmetric encryption algorithms, such as AES for example.

Algorithm 3: Algorithm for simulating the thresholds of the final quantum key length.

From the algorithm 1 that generate the quantum key length, the quantum key length will be known.

```
1: min=B;//big number, variable for minimum length of final quantum key length.
2: max=0;//variable for maximum length of final quantum key that share between the server and the IoT device.
3: for i:=N;//so big number to try the possible final quantum key length.
4:      if min> key[k]then
5:          min=key[k]
6:       if max<key[k]  then
7:           max=key[k]
```

Algorithm 3 defines the quantum key length thresholds for a number N of initial photons as the quantum key. The number of initial photons considered is 1000 (From Algorithm 1 that generates the quantum key length, the quantum key length will be known). At this stage, we assume that the test has been performed in a secure environment to guarantee that there is no attacker in the middle between the sender and the recipient.

In addition, the algorithm operates for a long time or the loop must be long enough to have the maximum and minimum quantum key length for a given number of initial photons. The loop used in this paper iterates over a million iterations. The attacker uses the polarization filter to detect the key length. Algorithm 4 reveals the

attacker's method for detecting the quantum key exchanged between the server and the IoT computer. In the beginning, we presume that the attacker has a few resources or capacity, so the attacker uses a fixed polarization filter, but then we assume that another attacker could adjust the polarization filter on demand (dynamic).

In line 10 the attacker is trying to capture the polarization of the photons. It is to be noted that, for a correct detection, the attacker should not only correctly use the same polarization of the photon transmitted by the sender but also this should be the polarization of the receiver filter. In fact, if the sender (Alice) and receiver (Bob) have used different polarizations, that bit will be discarded from the final key even if the attacker/eavesdropper (Eve) has used the same polarization of the photon that was sent from the source.

Algorithm 4: Simulation of the attacker (Man in the middle) used for fixed (static) polarization filter.

```
1: A[i];//From algorithm 1, the final key length at the receiver IoT device.
2: attacker[]=0;// declaration array for attacker detecting keys.
3: P=1;//for polarization filter.
4: for i:=Key length;//Final key length.
5:      attack [i]=p;//For saving the polarization filter.
6:      P=p+1;
7:      If p==4 then
8:          P==1;
9:   for k=Key length//final key length.
10:   If attacker[k]==A[k]&& attacker[k]==B[k] //A and B from the algorithm 1.
11:         detect==detect+1;
12:      Detected=Key length-detect;// the known key by the attacker.
```

5.2.2 The method for detecting an attacker.

This section describes an approach that can be applied regularly between sender and receiver in order to check if there is a man-in-the-middle attack. Thus, this is a "discovery" process to detect if there is an attacker, not an actual key generation process (but the attacker does not know this and would attempt to detect a "key").

In this approach, Alice and Bob will mimic the actual QKD process by transmitting a pre-agreed upon sequence of N photons where Bob knows the polarization filters to use. Consequently, in the absence of attack, the agreement between Alice and Bob should be for 100% of the photons. On the other hand, if an attacker (Eve) is present, it is extremely unlikely for her to guess 100% of the correct polarization filters, especially when N is large (in the results section we consider N=1000 for example).

Therefore, whenever she makes an incorrect guess and alters the photon polarization, this will be detected by Bob.

Algorithm 5 demonstrates this approach. The number of predicted photons at the receiver should be N, so a number significantly less than N means that an attacker is attempting to capture the key.

Algorithm 5: Algorithm for simulation the detection of an attacker (man in the middle).

```
1: attacker[]=0; // declaration array for attacker detecting keys.
2: attacked_ph = 0; // initialization of n of attacked photons
3: A[]=N;// the agreed of polarization photons ( e.g., N=1000) sent to Bob(B)
4: B[]=N;// the agreed of polarization photons (e.g., N=1000) received.
5: for i:=N;//the agreed photons number.
6:      If attacker[i]==A[i]&& attacker[i]==B[i].
7:         det_key[i]=A[i];// correctly detected by attacker
8: for k:=N;// number of agreed photons (e.g., N=1000)
9:       if B[k] !=A[k]//changed by the attacker due to wrong filter choice
10:         attacked_ph= attacked_ph+1//number of photons  attacked.
```

5.3 Results and discussion

Figure (16) shows the final key length that was generated for Controller number 1, the key length randomly generated for this time is 259, also the photon polarization is measured: we have 53 photons with a polarization of 0, 60 photons with a polarization of 45, 66 photons with a polarization of 90, and 66 photons with a polarization of 135 (the polarization numbers are random but by coincidence came in ascending order in this example).

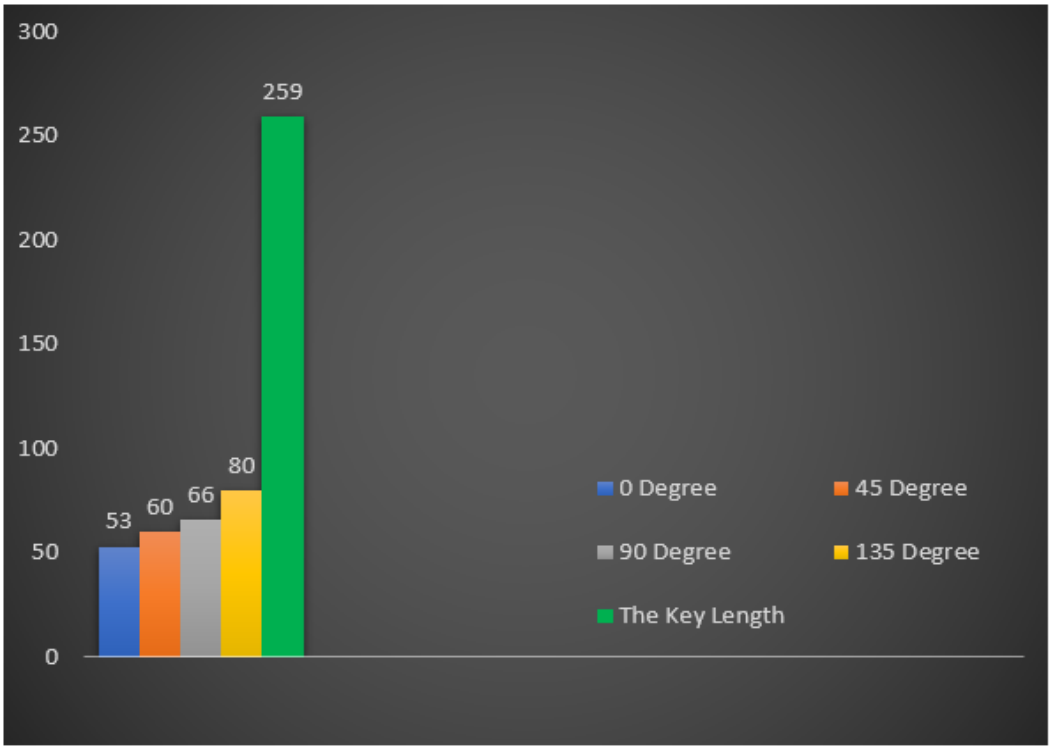


Figure 16:The key length and the polarization of each photon in the key for Controller 1.

Figure (17) indicates the final key length generated for Controller number 2, the key length generated randomly for this time is 238, also the photon polarization is measured: we have 57 photons with a polarization of 0, 48 photons with a polarization of 45, 67 photons with a polarization of 90, and 66 photons with a polarization of 135, and the random polarization is noticeable in Controller 2.

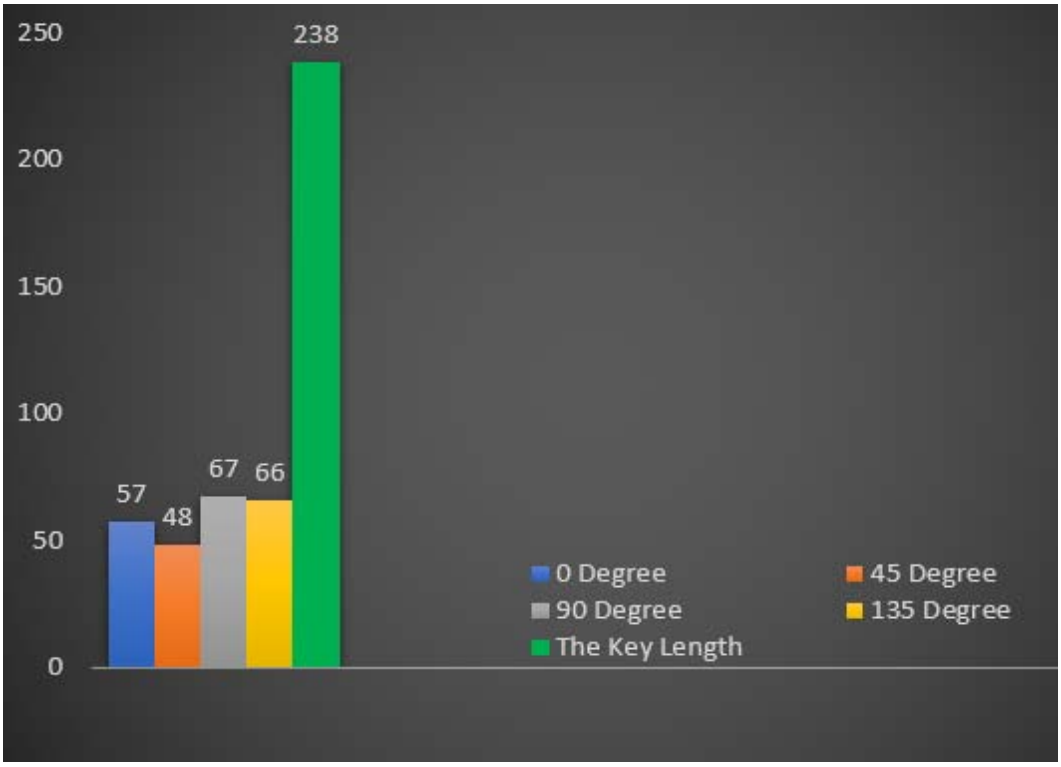


Figure 17: The key length and the polarization of each photon in the key for Controller 2.

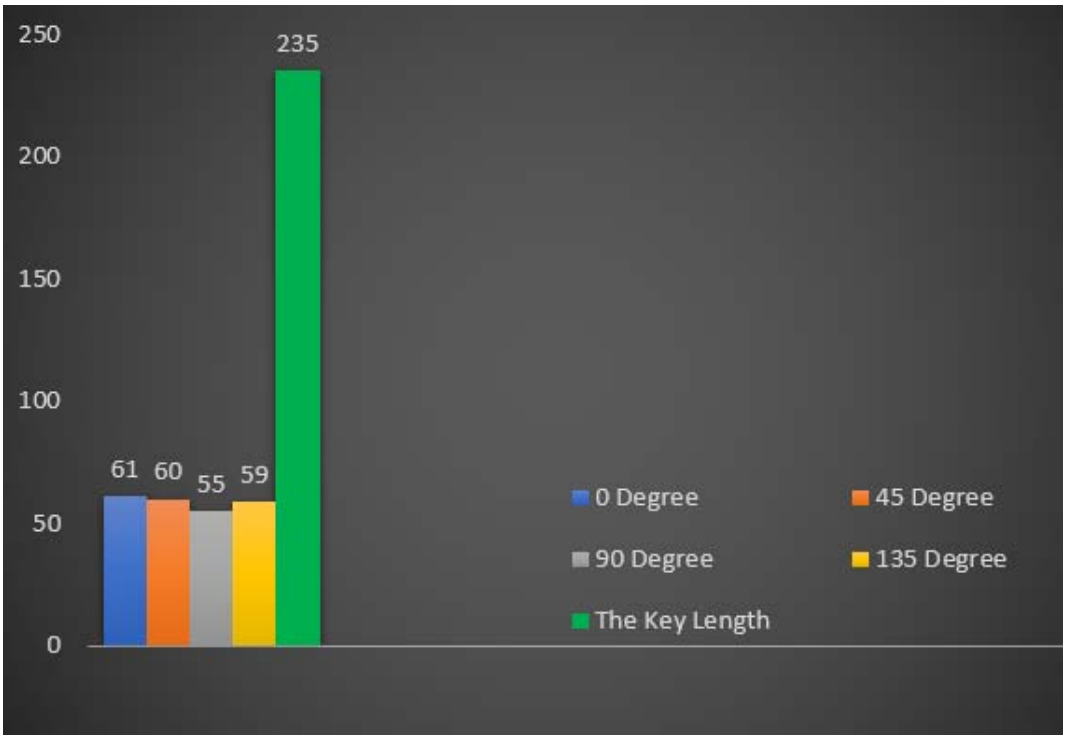


Figure 18: The key length and the polarization of each photon in the key for Controller 3.

Figure (18) displays the final key length generated for Controller number 3, the randomly generated key length for this time is 238, also the photon polarization is

measured: we have 61 photons with a polarization of 0, 60 photons with a polarization of 45, 55 photons with a polarization of 90, and 59 photons with a polarization of 135, where the random polarization is also evident in Controller 3.

5.3.2 Quantum key distribution in the presence of an attacker

In this section, we assume that each IoT device has an attacker to simulate the ability for the attacker to detect a certain length of the key. Figure 19 indicates the attackers simulated for each device and, in comparison, the number of key lengths securely obtained by each IoT device.

The thresholds of the quantum key length starting with 1000 initial photons (Qubit) are shown in Figure 19. Also, the figure indicates the same maximum number and the minimum number of potential key lengths that have been measured in a controlled environment; The maximum number of the final key length is 321, and the minimum number of the final key length is 188.

From Figure (19), the key length of device 1 is 259, the key length of device 2 is 238, and the key length of device 3 is 235, before the attack. After the attack, the securely exchanged key lengths (bits not detected correctly by the attacker) become 195, 203, and 204 for Devices 1, 2, and 3, respectively.

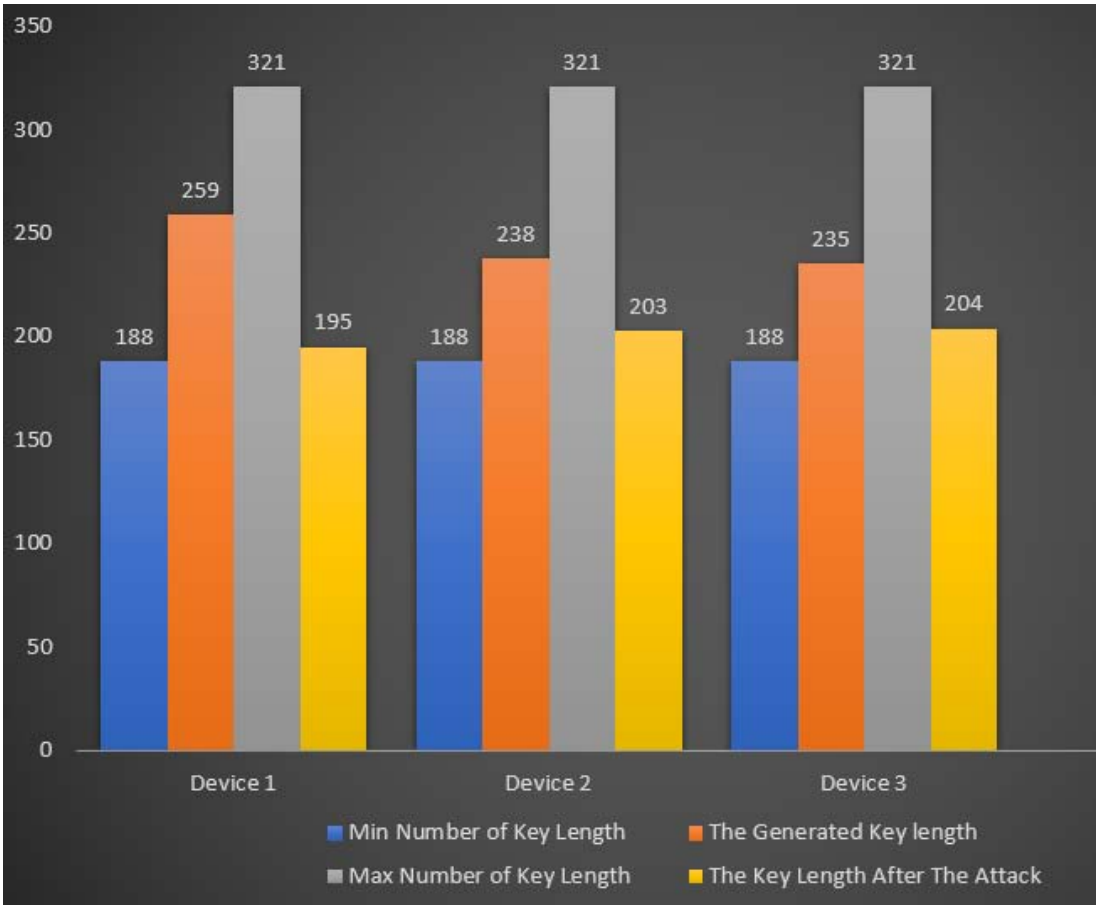


Figure 19: The thresholds, and the key length for each device after attacker (dynamic polarization filter).

It can be noted that these lengths are still longer than keys used in typical encryption algorithms, like AES where the length is 192 bits.

5.3.3 Attacker Detection

This section shows the implementation of Algorithm 5 between sender and receiver for checking if there is a man-in-the-middle attack. Alice and Bob will transmit a pre-agreed upon sequence of photons where Bob knows the polarization filters to use. As discussed previously, this is a "discovery" process to detect if there is an attacker, not an actual key generation process (but the attacker does not know). The amount of photons transmitted from the controller to the base station is seen in Figure

(20); the number of photons is N=1000; indeed, the number of photons and the polarization between the base station and the controller are accepted. In comparison, the number of photons correctly detected by the intruder is 251, and the number of photons arriving at the destination without changed polarization is 749. The sender and receiver will know that they have an attacker in the middle attempting to locate the transmitted key. Consequently, they will take this into account while trying to regenerate their actual key.

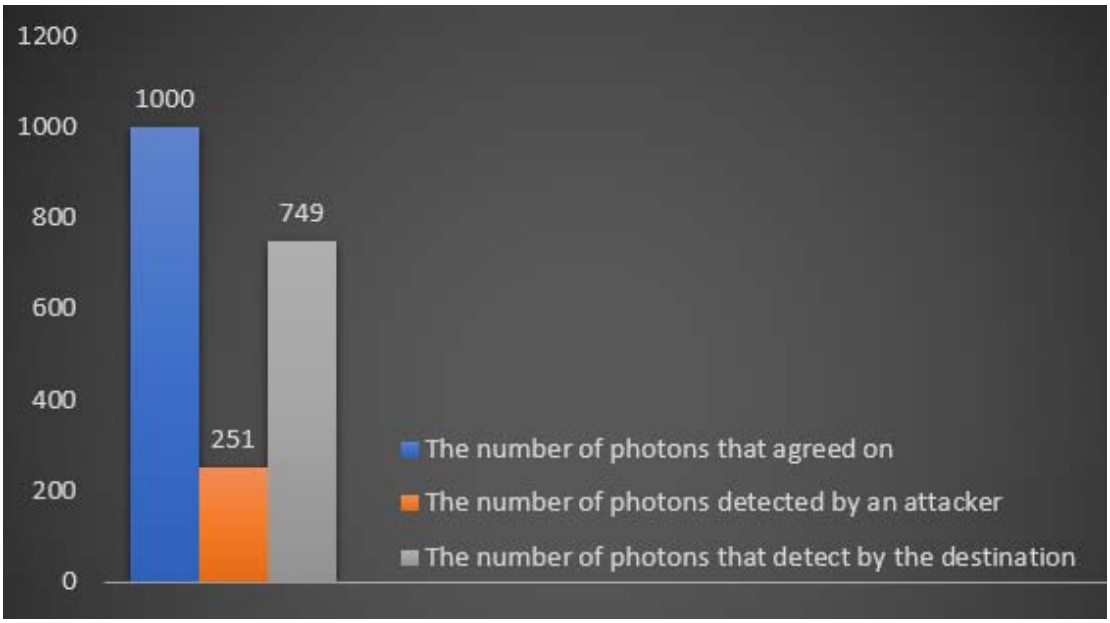


Figure 20: The number of agreed photons, the number of detected, and the number of photons at the destination.

CHAPTER 6: QUANTUM KEY DISTRIBUTION WITH MACHINE LEARNING.

Over the last ten years, there have been many significant advancements in the fundamental algorithms and techniques that have followed the rapid increase in functional implementations for machine learning [77]. Machine learning algorithms are categorized into two main types among some other categories which are out of our interest in this thesis. These types are Supervised, and Unsupervised learning algorithms based on the outcome of each algorithm. The unsupervised learning algorithms model the inputs dataset without providing the labels while supervised learning algorithms maps the input into the desired output by comparing with available label [78]. It can be formalized as a function inferring problem $y = f(\mathbf{x})$, based on a training set $\mathcal{D} = \{(\mathbf{x}_1, y_1), \dots, (\mathbf{x}_n, y_n)\}$. The inputs are d - dimensional vectors, $\mathbf{x}_i = \left[x_{i,1}, \dots, x_{i,d}\right]^T \in \mathbb{R}^d$. When y is continuous (e.g., $y \in \mathbb{R}$), in regression context, y is categorical nature (e.g., binary, $y \in \{-1,1\}$). The generalization of the obtained function is measured by how well it performs on new data expected to follow the same distribution as the training data [79]. A type of machine learning is the pattern recognition. This technology facilitates the learning process. As a result, it is an integral part of the whole machine learning technique. It enables algorithms to find regularities in large volumes of data and sort it into different categories. The information obtained from this pattern-searching can be utilized for analyzing the data system and providing a reliable answer for the critical decision making situations [80]. As the pattern recognition is considered part of machine learning, same machine learning algorithms can be used for this purpose, and for our work, we used two main supervised techniques, Neural Network, and support vector machine(SVM). The next subsection will explain each technique in detail and present the experiments results with performance evaluation.

6.1 Related work

This type of investigation, which has been suggested in this study, has never been performed before; all previous works have used machine learning in QKD for other implementations, but the proposed work is unique in detecting an attacker based on the final key length. This paragraph addresses similar work in general that used machine learning in QKD.

The realistic framework suggests an intelligent control technology based on optical spectrum analysis. An irregular optical spectrum signal can be automatically observed by using the linear discriminant analysis support vector machine algorithm through the machine learning-based optical spectrum analysis methodology, so as to understand attack identification and device intelligent monitoring.

Furthermore, the simulation and experimental results demonstrate that the linear discriminant analysis support vector machine algorithm can correctly distinguish the original spectral data and the irregular spectral data after the attack, and the qualified model can avoid the wavelength attacks well [81].

Different attack techniques undermine the functional security of a continuous-variable quantum key distribution (CVQKD) framework. Current countermeasures against these attacks are intended to take advantage of numerous real-time control modules to deter various forms of attacks, which are highly reliant on the precision of the estimated excess noise and lack a universal method of protection.

The authors suggest in [82] a security technique for CVQKD systems to overcome these limitations and to withstand the most recognized forms of attacks. they analyzed multiple pulse characteristics that would be influenced by various types of attacks, extract a feature vector based on these characteristics as an artificial neural

network (ANN) model input, and illustrated the ANN model's preparation and testing method for attack identification and classification. Simulation findings demonstrate that most of the known attacks can be detected successfully by the proposed scheme at the expense of reducing a limited portion of the hidden keys and transmission distance. By merely tracking many characteristics of the bursts without understanding the exact form of attack in advance, it sets up a universal attack detection model.

6.2 The method for detecting an attacker.

We used two types of supervised machine learning methods to detect an attacker, to ensure the accuracy and avoid the overfitting in the training.

6.2.1 Neural network pattern recognition.

Non-linear mathematical data structures that replicate the function of biological NNs are referred to as artificial neural networks (ANNs) which are considered the most widely studied and used approach for predictive patterns [83],[84]. In many challenges, ANN can effectively model complex or multi-complex tasks, as compared to traditional sequence approaches [85].

The generalization and learning capabilities of these networks are considered as a mathematical translation of biological neural networks. There are several applications of Neural networks in various areas, like finance, space education, sports and so on. This technique has been utilized to solve diagnosis, prediction and pattern recognition problems. When the relationship between the input and output is unknown or complex then this technique is perfectly suitable to be applied [86] .

The architecture of the neural network is simply consisting of three layers, the input layer where the data is received from the user, the hidden layer(s) which convert

the input data into a suitable form using specific parameters (weights and bias) to be used easily later by the output. The output layer is supposed to generate the final outcomes. All the layers are composed on basic nodes called neurons. The artificial neural networks have been classified into single layer feedforward neural network, multilayer feedforward network, recurrent network, or mesh network [87].

The main advantages of using the neural network technique are that they are a data-driven method that can process the data without any previous restrictions or back-knowledge assumptions about the model's form. Also, these techniques can learn by training on real data which make the model able to generalize on previously unseen data. The last advantage is due to processing the data using nonlinear activation function, this allows the network to detect the complex nonlinear type of relationships between the input and the output variables.

Mainly this type of machine learning techniques works on trial and error, so there is no specific structure or design that can work for all the problems. Basically, the network structure can be trained on the training part of the dataset then tested on the testing data and this process is repeated for a number of epochs and different parameters can be adjusted (like the number of hidden neurons and number of hidden layers) until reaching the least error obtained. In this case this model design will be selected [86].

One of the main neural networks types is the Multilayer Perceptron (MLP) that uses the multilayer feedforward architecture which is considered widely used for prediction and pattern recognition and it includes feedforward backpropagation, cascade feedforward backpropagation, and perception networks. To this thesis study, the feedforward backpropagation network was chosen based on the properties of the problem and the promising results obtained from our test.

For this thesis study, we did two different scenarios, the first one is to generate quantum keys without any attacker on their way (ideal situation), and for the second scenario, we added an attacker in the middle of their way. To confirm the outcomes of both scenarios, the first technique that was used to distinguish between attack keys and non-attack ones is Artificial Neural Network. The Neural Network Toolbox from MATALB was used for our test. This toolbox provides algorithms and pre-trained models, as well as applications for creating, training, visualizing, and simulating neural networks either with one hidden layer (called shallow neural network) or with multiple hidden layers called (deep learning neural networks). For our test, we used the shallow neural network to deal with the large dataset (around 20,000 sample). The structure of our network is as shown in Figure (21).

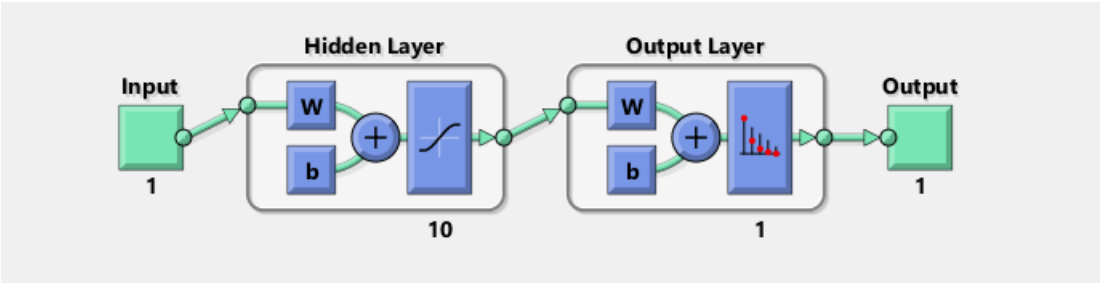


Figure 21: The structure of the neural network.

In our test, the learning algorithm was trained on 70% of the generated keys (training part) before being tested to predict either is it an attacker or not for each sample in the rest of the data set (test part). For each test set sample, a set of outcome probabilities should be assigned regarding to each of the attacker/non attacker groups—and the chosen group will be the one with highest probability. Here the test set is unseen and all the parameters adjustment was done during training to be used later, so in this case the overfitting issue was avoided to provide a robust performance estimation of the prediction.

6.2.2 Support Vector Machine (SVM).

The other technique which we used in this work is support vector machine (SVM) classifier. The fundamental principle of SVM is to find the decision surface that partitions the best vectors extracted from the data in vector space into two groups. This decision surface is known as the hyperplane that distinguishes between the two classes as shown in Figure (22) where the two classes are separated by the maximum margin [88].

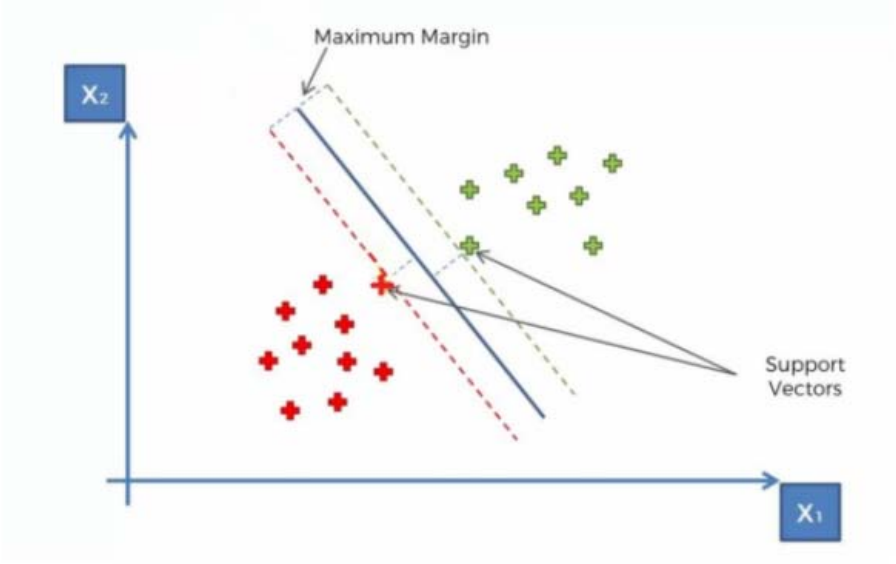


Figure 22: The hyperplane of SVM. [89]

As the dataset is a one-dimensional feature space, SVM was found to be utilized as the best algorithm because it mapped the input data into a high dimensional space. A decision surface, or hyperplane, is designed in this feature space. In the case of linearly separable data, this decision surface maximizes the "margin" between two groups (which means it has max distance from both classes. The sum of these two classes must be maximized to make this line as maximum margin). The unique attributes of this decision surface (hyperplane) guarantee the learning machine's high

generalization performance. The mathematical representation of this hyperplane is illustrated in the equation below.

$$\vec{w}\vec{x} + b = 0 \quad (6.1)$$

Where:

Vector W and constant b are the learned parameters from the training dataset.

Vector x is the datapoint.

The SVM transfer the dataset to a high dimensional space based on the concept of Kernel trick to compute the inner products between all pairs of data in the feature space. There is no need to explicitly increase the dimension by explicitly transforming into feature vector representations in higher space.

6.3. Performance evaluation metrics

Four traditional assessment metrics, namely: accuracy, F1 score, precision and recall, were chosen. Any of these metrics is determined using the True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN) values calculated and represented by the uncertainty matrix throughout the test process. For a binary classification query, Table 8 shows the general confusion matrix.

Table 8: Binary Classification Confusion Matrix

		Predicted	
		Positive	Negative
Actual	Positive	TP	FN
	Negative	FP	TN

Any of the chosen metrics will offer some insights into the model's results, which will strengthen the assessment process. A brief overview of each is shown below:

- **Accuracy:** The ratio of accurate predictions to the total number of predictions is calculated. This can be measured in a binary hierarchy as:

$$\text{Accuracy} = \frac{TP + TN}{TP+TN+FN+FP} \quad (6.2)$$

- **Precision:** The ratio between the correctly expected data and the overall optimistic predicted details. This ensures that a high-precision model is capable of accurately defining much of the expected results (see equation 6.3).

$$\text{Precision} = \frac{TP}{TP + FP} \quad (6.3)$$

- **Recall:** This metric gives an analysis of the model's sensitivity. That is, the percentage of the positive data that was accurately defined as positive and the positive total data (see equation 6.4).

$$\text{Recall} = \frac{TP}{TP + FN} \quad (6.4)$$

- **F1 score**: Using precision and recall, the forth evaluation metric is calculated using Equation 6.5.

$$\text{F1\_Score} = 2 * \frac{Recall * Precision}{Recall + Precision} \quad (6.5)$$

The F1 score is used to demonstrate the model's overall success in relation to both accuracy and recall. The benefit of using the F1 score for assessing a model's overall success is that the F1 score takes into account the distribution of data and the unequal class situation where false positive and false negative are at stake, which is typically the case with all the algorithms.

6.4 Results and discussion

The results are showed in the two parts below.

6.4.1 Neural Network

The network was trained for 1000 epochs with data splitting of 70% training part, 15% validation part and 15% testing part, to test for algorithm's robustness against any bias towards data split.

Table(9) below shows the results of the evaluation metrics mentioned above.

Table 9:The evaluation metrics.

Dataset- split	Accuracy	Precision	Recall	F1-score
70%-30%	99.1%	98.8%	99.3%	99.04

Figure(23) below shows the performance plot for the data set:

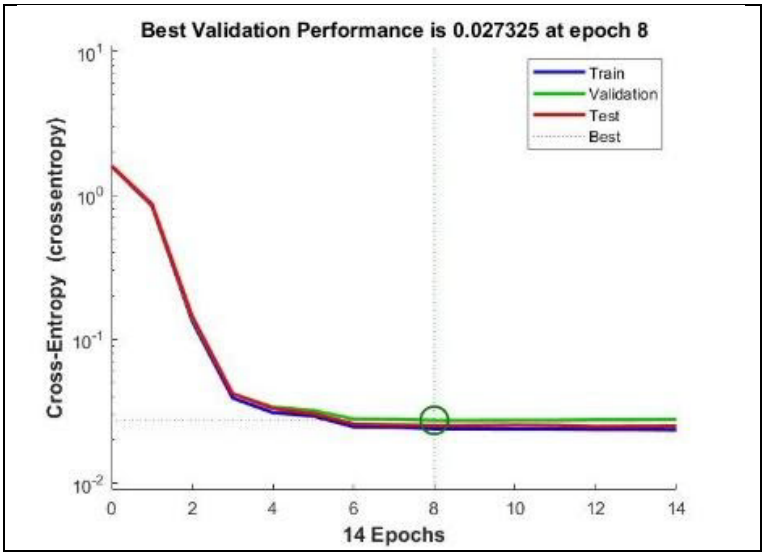
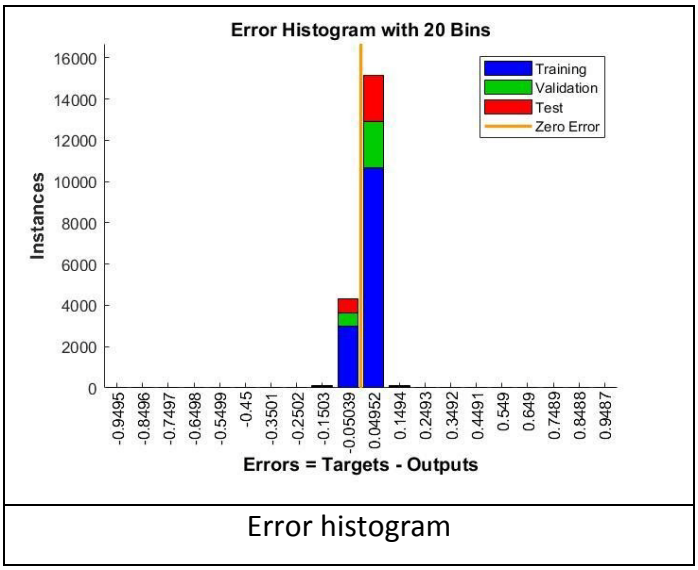


Figure 23: the performance plot of the classification test.

The performance plot represents the relationship between the cross-entropy loss which measures the performance of the classification model and the number of epochs. It is clear from the graph that a significant decrease in error between the target and the measured output for training, validation and testing partitions of the dataset is noted to almost reach zero. This result is also confirmed by the histogram error graph (see Figure 24), where it shows the test set bar and the train set bar around the zero-error

rate.



Error histogram

Figure 24: the histogram error graph.

6.4.2 Support Vector Machine.

The dataset is only one dimension; therefore, the scatter plot will not work and to make it work, we need to add dummy variable such that we can plot using scatter plot and train using SVM. The distribution of our dataset is represented as shown in Figure (25).

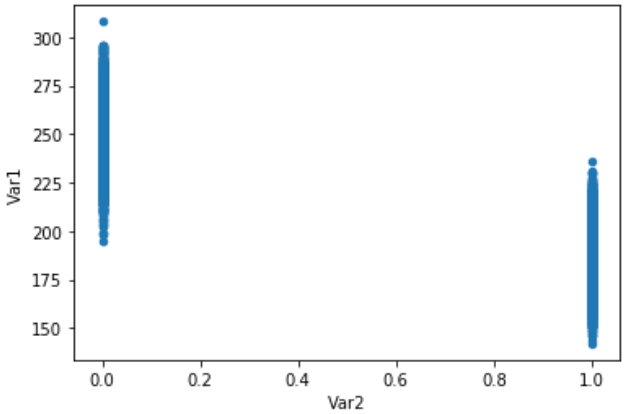


Figure 25: The distribution of dataset.

Where Var1 is the generated keys and Var2 is the class. For training, we used a polynomial kernel to train the SVM after splitting the dataset into 70% train and 30% test, the result is as shown in Table (10), and Figures (26, and 27), where “0”

corresponds to the QKD without attacker, and “1” with the attacker effect.

Table 10: The accuracy results for testing model in SVM.

	Precision	Recall	F1-score	Support
0	0.99	0.99	0.99	3010
1	0.99	0.99	0.99	2990
Accuracy	0.99	0.99	0.99	6000

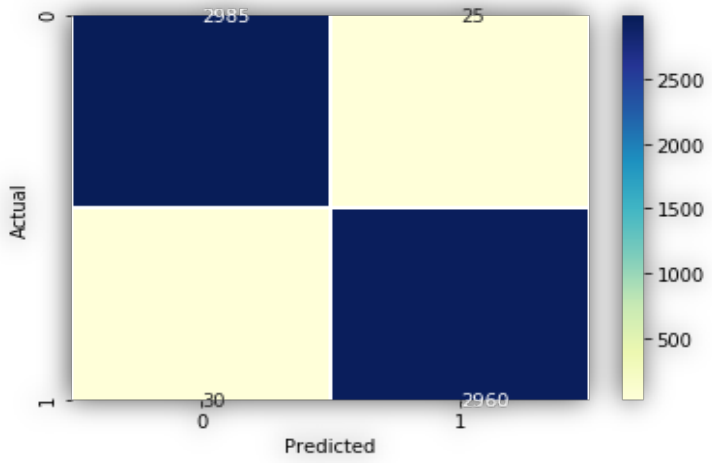


Figure 26: The correlation between the actual result and the predicted one.

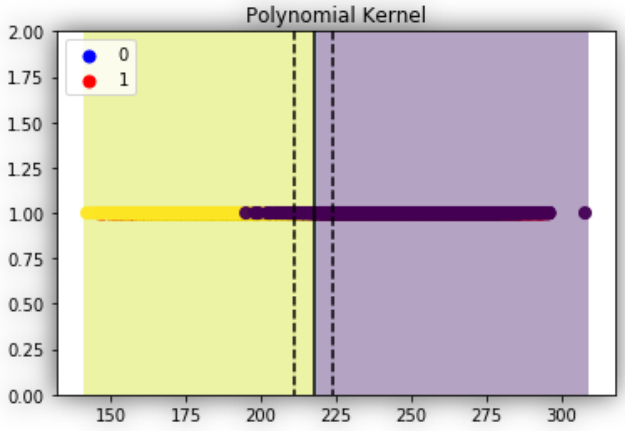


Figure 27: The results after classification by SVM.

It is clear from the classification results that we obtained high accuracy referring

to the high integrity and confidentiality while transferring the photons, and the small error that appeared is negligible. This result is promising and proved our goal from this test. There is no overfitting because we already did different experiments by using other machine learning algorithms as well as using another type of SVM kernels. And all the results showed as close as to the current accuracy.

6.5 The effect of increasing the initial photons.

We need to quantify the effect of raising the initial photons that are sent by the server on the final key length that arrive at the destination, in our case the IoT devices. In this thesis we used several initial photons and compared with the corresponding final key length, the initial photons were increasing from just 10 photons up to 1000,000 initial photons.

On another hand, the final key length was determined for corresponding initial photons, then we compared them. Moreover, in this process, we show the versatility of the proposed method how it can easily produce any needed initial photons even if the request of the initial photons is a massive number.

After detecting an attacker that is trying to get a key in the middle, the two parties who want to distribute a key can make the initial photons mire the last to make detecting the key harder for the attacker, regarding the Figure (28) that has shown the correlation between the initial photons that are sent by the server, the final key will increase more than expected.

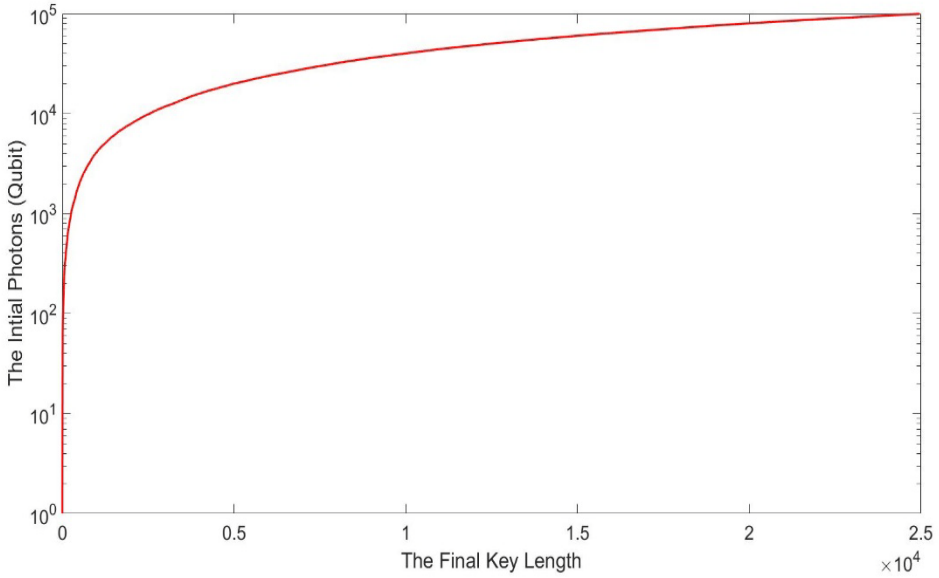


Figure 28: The correlation between increasing of the intial photons and the final key length.

Figure (28) illustrates the number of initial sending photons versus the final key length. It is apparent that increasing the number of the sent photons will raise the final key length, but the figure shows this increase in a way not to be expected. For example, for the initial number of 1000 photons, the final key length will be up to 322 in the best case. In this way we can estimate that when sending 2000 photons the final key length will be 644 in the best case, but this is not the calculation: We can see from the figure the final key length will be more than 700 in case of 2000 initial photons, and so on and so forth. In this way, after detecting an attacker by the proposed method we can be raising the number of the initial photons.

CHAPTER 7: CONCLUSION AND FUTURE WORK

The thesis proposed a novel method for simulating quantum key distribution between server and IoT controllers for securing the communication, generating and measuring the final key length for the specified number of initial photons, and for using the final key for symmetrical encryption to ensure data protection for IoT devices.

Moreover, the performance under a man in the middle attacker was addressed in the simulations. The final key exchanged with this quantum approach is of sufficient length to be used in symmetric cryptography, such as the AES algorithm, by IoT devices, even in the presence of the attacker. Also, machine learning techniques were used to predict the presence of an attacker during quantum key distribution.

The quantum satellite communications are emerging within the prospect of the quantum age, therefore they constitute an interesting direction for future study. Another topic for future study is using QKD with asymmetric cryptography for securing the transmission for long-distance communications.

PUBLICATIONS

[1] Hasan Abbas Al-Mohammed and Elias Yaacoub, “New Way to Generating and Simulation QKD.,” *6th Int. Congr. Inf. Commun. Technol.*, 2021. (accepted).

[2] Hasan Abbas Al-Mohammed and Elias Yaacoub, “A Novel Way for Simulating and Generating Quantum Key Distribution with Machine Learning for Securing IoT Devices and detecting attacker by using Machine learning.,” *Int. J. Quantum Inf.*, 2021.(submitted)

[3] Hasan Abbas Al-Mohammed., “Quantum Cryptography in real-life applications,” in *Emerging Paradigm 2021*, Wiley, 2021. (accepted abstract).

[4] Hasan Abbas Al-Mohammed. Elias Yaacoub, “On the Use of Quantum Communications for Securing IoT Devices in the 6G Era.,” *IEEE Int. Conf. Commun. / Montr. Connect. – Secur. – Priv.*, 2021.(submitted).

[5] Hasan Abbas Al-Mohammed., “Quantum computer architecture from non-conventional physical simulation up to encryption cracking, machine learning application, and more,” *IEEE Int. Conf. ICENCO.*, 2021. (published).

[6] Hasan Abbas Al-Mohammed, “Quantum Radar A Brief Analytical Study.,” *IEEE Int. Conf. ICENCO*, 2021. (published).

[7] Hasan Abbas Al-Mohammed, “Quantum Communication Methods Based On The Nodes ’ Connectivity,” *Int. J. Eng. Res. Electron. Commun. Eng.*, vol. 7, no. 11, pp. 24–29, 2020. (published).

REFERENCES

[1] H. Viswanathan and P. E. Mogensen, “Communications in the 6G Era,” *IEEE Access*, vol. 8, pp. 57063–57074, 2020, doi: 10.1109/ACCESS.2020.2981745.

[2] O. L. A. Lopez, H. Alves, R. D. Souza, S. Montejo-Sanchez, E. M. G. Fernandez, and M. Latva-aho, “Massive Wireless Energy Transfer: Enabling Sustainable IoT Towards 6G Era,” *IEEE Internet Things J.*, vol. 4662, no. 11200659, pp. 1–19, 2021, doi: 10.1109/JIOT.2021.3050612.

[3] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, “Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook,” *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 881–919, 2019, doi: 10.1109/COMST.2018.2864557.

[4] E. Coronas, D. Version, and E. Coronas, “Delft University of Technology Quantum internet The internet’s next big step,” 2019.

[5] A. S. Holevo and V. Giovannetti, “Quantum channels and their entropic characteristics,” *Reports Prog. Phys.*, vol. 75, no. 4, 2012, doi: 10.1088/0034-4885/75/4/046001.

[6] R. Asif, “Future Quantum-to-the-Home (QTTH) All-Optical Networks (Invited Talk),” *2018 10th Int. Conf. Adv. Infocomm Technol.*, pp. 41–46, 2018.

[7] S. Imre and L. Gyongyosi, *Advanced Quantum Communications*. 2013.

[8] P. Van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, “Quantum repeaters using coherent-state communication,” *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 78, no. 6, pp. 1–11, 2008, doi: 10.1103/PhysRevA.78.062319.

[9] G. Brassard, “Quantum communication complexity,” *Found. Phys.*, vol. 33, no. 11, pp. 1593–1616, 2003, doi: 10.1023/A:1026009100467.

[10] S. K. Liao *et al.*, “Satellite-Relayed Intercontinental Quantum Network,” *Phys. Rev. Lett.*, vol. 120, no. 3, p. 30501, 2018, doi: 10.1103/PhysRevLett.120.030501.

[11] T. Jennewein, “Towards Quantum Communications with Satellites,” *IEEE Photonics Soc. Summer Top. Meet. Ser. SUM 2018*, pp. 217–218, 2018, doi: 10.1109/PHOSST.2018.8456781.

[12] C. Li *et al.*, “Quantum Communication between Multiplexed Atomic Quantum Memories,” pp. 1–9, 2019, [Online]. Available: http://arxiv.org/abs/1909.02185.

[13] L. H. Shi, X. T. Yu, X. F. Cai, Y. X. Gong, and Z. C. Zhang, “Quantum information transmission in the quantum wireless multihop network based on Werner state,” *Chinese Phys. B*, vol. 24, no. 5, p. 050308, 2015, doi:

10.1088/1674-1056/24/5/050308.

[14] C. Cai, Y. Sun, Y. Zhang, P. Zhang, J. Niu, and Y. Ji, “Experimental wavelength-space division multiplexing of quantum key distribution with classical optical communication over multicore fiber,” *Opt. Express*, vol. 27, no. 4, p. 5125, 2019, doi: 10.1364/oe.27.005125.

[15] S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola, “Microwave quantum illumination,” *Phys. Rev. Lett.*, vol. 114, no. 8, pp. 1–5, 2015, doi: 10.1103/PhysRevLett.114.080503.

[16] S. Zhao, “Quantum detection theory and optimum strategy in quantum radar system,” no. Irc 2018, pp. 2–5, 2019, doi: 10.1049/joe.2019.0631.

[17] R. Jantti, R. Duan, J. Lietzen, H. Khalifa, and L. Hanzo, “Quantum-Enhanced Microwave Backscattering Communications,” *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 80–85, 2020, doi: 10.1109/MCOM.001.1900112.

[18] P. W. Evans, “The End of a Classical Ontology for Quantum Mechanics?,” *Entropy*, vol. 23, no. 1, p. 12, 2020, doi: 10.3390/e23010012.

[19] S. Khatri, A. J. Brady, and M. P. Bart, “Spooky action at a global distance analysis of space-based entanglement distribution for the quantum internet,” *npj Quantum Inf.*, 2021, doi: 10.1038/s41534-020-00327-5.

[20] D. Gries and F. B. Schneider, *Explorations in Quantum Computing*, 2nd ed. Springer, 2020.

[21] G. Lindblad, “A general no-cloning theorem,” *Lett. Math. Phys.*, vol. 47, no. 2, pp. 189–196, 1999, doi: 10.1023/A:1007581027660.

[22] W. H. W. K. Wootters, Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, 1982, doi: 10.1038/246170a0.

[23] F. Ming, D. Wang, X.-G. Fan, W.-N. Shi, L. Ye, and J.-L. Chen, “Improved tripartite uncertainty relation with quantum memory,” *arXiv*, no. 3, pp. 1–7, 2020, [Online]. Available: http://arxiv.org/abs/2004.04356.

[24] F. P. Mezzapesa, L. L. Columbo, M. Brambilla, M. Dabbicco, M. S. Vitiello, and G. Scamarcio, “Imaging of free carriers in semiconductors via optical feedback in terahertz quantum cascade lasers,” *Appl. Phys. Lett.*, vol. 104, no. 4, pp. 0–1, 2014, doi: 10.1063/1.4863671.

[25] Y. T. Aladadi, A. F. Abas, A. Alwarafy, and M. T. Alresheedi, “Multi-user frequency-time coded quantum key distribution network using a plug-and-play system,” *22nd Conf. Opt. Netw. Des. Model. ONDM 2018 - Proc.*, pp. 53–58, 2018, doi: 10.23919/ONDM.2018.8396106.

[26] S. Imre, “Quantum communications: Explained for communication engineers,”

IEEE Commun. Mag., vol. 51, no. 8, pp. 28–35, 2013, doi: 10.1109/MCOM.2013.6576335.

[27] Gartner, “Gartner.” https://www.gartner.com/en (accessed Mar. 04, 2021).

[28] “Google trends,” *Google*. https://trends.google.com/trends/?geo=US (accessed Mar. 04, 2021).

[29] B. Zygelman, *A First Introduction to Quantum Computing and Information*. Springer International Publishing, 2018.

[30] D. P. DiVincenzo, “The physical implementation of quantum computation,” *Fortschritte der Phys.*, vol. 48, no. 9–11, pp. 771–783, 2000, doi: 10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E.

[31] R. Van Meter and C. Horsman, “A blueprint for building a quantum computer,” *Commun. ACM*, vol. 56, no. 10, pp. 84–93, 2013, doi: 10.1145/2494568.

[32] A. V. Dastjerdi and R. Buyya, “Fog Computing: Helping the Internet of Things Realize Its Potential,” *Computer (Long. Beach. Calif).*, vol. 49, no. 8, pp. 112–116, 2016, doi: 10.1109/MC.2016.245.

[33] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, “A survey of machine and deep learning methods for internet of things (IoT) security,” *IEEE Commun. Surv. TUTORIALS*, vol. 22, no. 3, pp. 1646–1685, 2020.

[34] E. Yaacoub and M. S. Alouini, “A Key 6G Challenge and Opportunity--Connecting the Base of the Pyramid: A Survey on Rural Connectivity,” *Proc. IEEE*, vol. PP, pp. 1–50, 2020, doi: 10.1109/JPROC.2020.2976703.

[35] T. M. Fernandez-Carames, “From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things,” *IEEE Internet Things J.*, vol. 7, no. 7, pp. 1–1, 2019, doi: 10.1109/jiot.2019.2958788.

[36] E. Yaacoub, K. Abualsaud, T. Khattab, and A. Chehab, “Secure Transmission of IoT mHealth Patient Monitoring Data from Remote Areas Using DTN,” *IEEE Netw.*, vol. 34, no. 5, pp. 226–231, 2020, doi: 10.1109/MNET.011.1900627.

[37] S. K. Singh, A. El Azzaoui, M. M. Salim, and J. H. Park, “Quantum Communication Technology for Future ICT - Review,” *J. Inf. Process. Syst.*, vol. 16, no. 6, pp. 1459–1478, 2020, doi: 10.3745/JIPS.03.0154.

[38] B. Zohuri, *Radar Energy Warfare and the Challenges of Stealth Technology*. 2020.

[39] H.Klinkrad, *Models and Risk Analysis*. Springer-Praxis, 2006.

[40] F. Daum, “Quantum Radar Cost and Practical Issues,” *IEEE Aerosp. Electron.*

Syst. Mag., vol. 35, no. 11, pp. 8–20, 2020, doi: 10.1109/MAES.2020.2982755.

[41] A. Pérez-Salinas, J. Cruz-Martinez, A. A. Alhajri, and S. Carrazza, "Determining the proton content with a quantum computer," *Phys. Rev. D*, vol. 103, no. 3, p. 034027, 2021, doi: 10.1103/PhysRevD.103.034027.

[42] C. Chareton, S. Bardin, F. Bobot, V. Perrelle, and B. Valiron, "Toward certified quantum programming," *arXiv Prepr. arXiv2003.05841*, 2020, [Online]. Available: http://arxiv.org/abs/2003.05841.

[43] G. Vallone *et al.*, "Experimental Satellite Quantum Communications," *Phys. Rev. Lett.*, vol. 115, no. 4, pp. 1–5, 2015, doi: 10.1103/PhysRevLett.115.040502.

[44] H. Dai *et al.*, "Towards satellite-based quantum-secure time transfer," *Nat. Phys.*, vol. 16, no. 8, pp. 848–852, 2020, doi: 10.1038/s41567-020-0892-y.

[45] C. L. Degen, F. Reinhard, and P. Cappellaro, "Quantum sensing," *Rev. Mod. Phys.*, vol. 89, no. 3, pp. 1–39, 2017, doi: 10.1103/RevModPhys.89.035002.

[46] D. Carney *et al.*, "Mechanical quantum sensing in the search for dark matter," *Quantum Sci. Technol.*, vol. 6, no. 2, pp. 1–19, 2021, doi: 10.1088/2058-9565/abcfcd.

[47] A. Broadbent and C. Schaffner, *Quantum cryptography beyond quantum key distribution*, vol. 78, no. 1. 2016.

[48] R. Di Candia, H. Yiğitler, G. S. Paraoanu, and R. Jäntti, "Two -way covert microwave quantum communication," *arXiv*. 2020.

[49] S. Pirandola, B. R. Bardhan, T. Gehring, C. Weedbrook, and S. Lloyd, "Advances in photonic quantum sensing," *Nat. Photonics*, vol. 12, no. 12, pp. 724–733, 2018, doi: 10.1038/s41566-018-0301-6.

[50] Y. Hashimoto, *Recent Developments in Multivariate Public Key Cryptosystems*. Springer, Singapore., 2021.

[51] F. Regazzoni, "Post-Quantum Lattice-Based Cryptography Implementations: A Survey," *ACM Comput. Surv.*, vol. 51, no. 6, 2019.

[52] H. C. Prithvik, K. R. Charan, B. S. Sachin, and K. R. Rakesh, "Implementation of Quantum Key Distribution using Python," *Wutan Huatan Jisuan Jishu*, vol. XVI, no. 190, pp. 190–196, 2020.

[53] A. . and Ms.Krithika.S, "Implementation of BB84 Quantum Key Distribution using OptSim.," in *IEEE sponsere, INTERNATIONAL CONFERENCE ON ELECTRONICS AND COMMUNICATION SYSTEM (ICECS 2015) Implementation*, 2015, no. Icecs, pp. 457–460.

[54] D. Bruss, G. Erdélyi, T. Meyer, T. Riege, and J. Rothe, "Quantum

cryptography: A survey," *ACM Comput. Surv.*, vol. 39, no. 2, pp. 6-es, 2007, doi: 10.1145/1242471.1242474.

[55] M. Sasaki, "Quantum key distribution and its applications," *IEEE Secur. Priv.*, vol. 16, no. 5, pp. 42–48, 2018, doi: 10.1109/MSP.2018.3761713.

[56] B. Muruganantham, P. Shamili, S. Ganesh Kumar, and A. Murugan, "Quantum cryptography for secured communication networks," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, pp. 407–414, 2020, doi: 10.11591/ijece.v10i1.pp407-414.

[57] F. Editors *et al.*, *Applied Quantum Cryptography ,Lecture Notes in Physics, (Vol. 797).*, 1st edn. Springer Berlin Heidelberg, 2010.

[58] H. Zhang, Z. Ji, H. Wang, and W. Wu, "Survey on quantum information security," *China Commun.*, vol. 16, no. 10, pp. 1–36, 2019, doi: 10.23919/JCC.2019.10.001.

[59] A. A. A. El-Latif *et al.*, "Providing End-to-End Security Using Quantum Walks in IoT Networks," *IEEE Access*, vol. 8, pp. 92687–92696, 2020, doi: 10.1109/ACCESS.2020.2992820.

[60] H. Singh, D. L. Gupta, and A. . Singh, "Quantum Key Distribution Protocols: A Review," *IOSR J. Comput. Eng.*, vol. 16, no. 2, pp. 01–09, 2014, doi: 10.9790/0661-162110109.

[61] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, 2000, doi: 10.1103/PhysRevLett.85.441.

[62] A. A. Amusan and E. A. Amusan, "Design and Simulation of 1.28 Tbps Dense Wavelength Division Multiplex System Suitable for Long Haul Backbone," *J. Opt. Commun.*, 2018, doi: 10.1515/joc-2018-0156.

[63] M. E. System, "using OptSim," *IEEE sponsere, Int. Conf. Electron. Commun. Syst. (ICECS 2015) Implement.*, no. Icecs, pp. 457–460, 2015.

[64] J. R. Johansson, P. D. Nation, and F. Nori, "QuTiP: An open-source Python framework for the dynamics of open quantum systems," *Comput. Phys. Commun.*, vol. 183, no. 8, pp. 1760–1772, 2012, doi: 10.1016/j.cpc.2012.02.021.

[65] Dr C R S Kumar, "Quantum Key Distribution using Simulink Fuzzy Logic Quantum Key Distribution Modelling using Simulink Results," no. April, pp. 1–30, 2015, [Online]. Available: https://www.mathworks.com/content/dam/mathworks/mathworks-dot-com/solutions/automotive/files/in-expo-2015/modelling-fuzzy-logic-quantum-key-distribution-using-simulink.pdf.

[66] A. P. Y. A. R. A. Atashpendar, "QKD simulator, Homepage,

https://www.qkdsimulator.com/, Last visit Jan 2021."

[67] A. Mavromatis, F. Ntavou, E. H. Salas, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Experimental Demonstration of Quantum Key Distribution (QKD) for Energy-Efficient Software-Defined Internet of Things," *Eur. Conf. Opt. Commun. ECOC*, vol. 2018-Septe, no. 1, pp. 1–3, 2018, doi: 10.1109/ECOC.2018.8535267.

[68] H. D. He Z, Wang Y, "Wavelength attack recognition based on machine learning optical spectrum analysis for the practical continuous-variable quantum key distribution system." pp. 1689–1697, 2020.

[69] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, 2014, doi: 10.1016/j.jnca.2014.01.014.

[70] S. Ray, Y. Jin, and A. Raychowdhury, "The Changing Computing Paradigm with Internet of Things: A Tutorial Introduction," *IEEE Des. Test*, vol. 33, no. 2, pp. 76–96, 2016, doi: 10.1109/MDAT.2016.2526612.

[71] D. Evans, "How the Next Evolution of the Internet Is Changing Everything," *Cisco Internet Bus. Solut. Gr.*, no. April, 2011, [Online]. Available: http://115.112.165.74:81/Krishna Akalamkam/digital marketing/articles/The Internet of Things_.pdf.

[72] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks," *J. Cyber Secur. Mobil.*, vol. 4, no. 1, pp. 65–88, 2015, doi: 10.13052/jcsm2245-1439.414.

[73] A. Lohachab, A. Lohachab, and A. Jangra, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks," *Internet of Things*, vol. 9, no. Mar, p. 100174, 2020, doi: 10.1016/j.iot.2020.100174.

[74] M. Mehic, O. Maurhart, S. Rass, and M. Voznak, "Implementation of quantum key distribution network simulation module in the network simulator NS-3," *Quantum Inf. Process.*, vol. 16, no. 10, pp. 1–23, 2017, doi: 10.1007/s11128-017-1702-z.

[75] N. Y. Philip *et al.*, "Internet of Things for In-Home Health Monitoring Systems : Current Advances , Challenges and Future Directions," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 300–310, 2021.

[76] I. Ullah, N. U. Amin, M. A. Khan, H. Khattak, and S. Kumari, "An Efficient and Provable Secure Certificate-Based Combined Signature, Encryption and Signcryption Scheme for Internet of Things (IoT) in Mobile Health (M-Health) System," *J. Med. Syst.*, vol. 45, no. 1, pp. 1–14, 2021, doi: 10.1007/s10916-020-01658-8.

[77] C. M. Bishop, *Pattern recognition and machine learning*. springer, 2006.

[78] T. O. Ayodele, “Types of Machine Learning Algorithms,” *New Adv. Mach. Learn.*, vol. 3, pp. 19–48, 2010, doi: 10.5772/9385.

[79] M. A. T. Figueiredo, “Adaptive sparseness for supervised learning,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 9, pp. 1050–1159, 2003, doi: 10.1109/TPAMI.2003.1227989.

[80] Z. Gimon, “What Is Pattern Recognition in Machine Learning,” 2019. https://huspi.com/blog-open/pattern-recognition-in-machine-learning (accessed Mar. 05, 2021).

[81] H. D. He Z, Wang Y, “Wavelength attack recognition based on machine learning optical spectrum analysis for the practical continuous-variable quantum key distribution system,” *JOSA B*, vol. 37, no. 6, pp. 1689–1697, 2020.

[82] Y. Mao *et al.*, “Detecting quantum attacks: A machine learning based defense strategy for practical continuous-variable quantum key distribution,” *New J. Phys.*, vol. 22, no. 8, 2020, doi: 10.1088/1367-2630/aba8d4.

[83] and K. M. M. Jain, Anil K., Jianchang Mao, “Artificial neural networks: a tutorial,” *Computer (Long. Beach. Calif).*, vol. 29, no. 3, pp. 31–44, 1996.

[84] H. Y. Priyangga and D. Ruliandi, “Application of Pattern Recognition and Classification Using Artificial Neural Network in Geothermal Operation,” *Stanford Univ*, pp. 1–9, 2018.

[85] L. Lazli and M. Boukadoum, “Hidden Neural Network for Complex Pattern Recognition: A Comparison Study with Multi- Neural Network Based Approach,” *Int. J. Life Sci. Med. Res.*, vol. 3, no. 6, pp. 234–245, 2013, doi: 10.5963/lsmr0306003.

[86] M. Şahin and R. Erol, “A Comparative Study of Neural Networks and ANFIS for Forecasting Attendance Rate of Soccer Games,” *Math. Comput. Appl.*, vol. 22, no. 4, p. 43, 2017, doi: 10.3390/mca22040043.

[87] I. N. da Silva, D. H. Spatti, R. A. Flauzino, L. H. B. Liboni, and S. F. dos Reis Alves, “Artificial neural networks: A practical course,” in *Artificial Neural Networks*, Switzerland: Springer International Publishing, 2017, pp. 21–27.

[88] M. V. Kotpalliwar and R. Wajgi, “Classification of attacks using support vector machine (SVM) on KDDCUP’99 IDS database,” in *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, 2015, pp. 987–990, doi: 10.1109/CSNT.2015.185.

[89] AQSAZAFAR, “SVM machine learning,” 2020. https://

www.mltut.com/svm-machine-learning/ (accessed Mar. 05, 2021).