ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/345675328

Quantum Cryptography

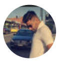
Thesis · November 2020

DOI: 10.13140/RG.2.2.34447.61601

CITATIONS
2

READS
14,489

1 author:



Maneesh Yati
Deakin University

3 PUBLICATIONS **2** CITATIONS

SEE PROFILE

All content following this page was uploaded by Maneesh Yati on 10 November 2020.

The user has requested enhancement of the downloaded file.

Minor Thesis

Quantum Leap

Thesis – "Quantum Cryptography"

DEAKIN UNIVERSITY

Author: Maneesh Yati

Supervised By:

Dr Alessio Bonti,
Dr Amani Ibrahim

Contents

Abstract:

History of computing can be simplified into 19th century in which computing used to be a mental process, 20th century machine process and in 21st century it is thought of nature's way of computing or "quantum computing". Since 1970's when Richard Feynman proposed the idea of simulating the evolution of quantum system(Feynman 1986), there has been substantial development in the field of Quantum computing but there was not enough evidence to prove that Quantum computers really exist. The biggest achievement in the field of quantum computing is that scientist have made a quantum computer which exist in real world, earlier everything was theoretical. Quantum computers are at its verge to disrupt the computation technology. Quantum computers offer huge possibilities for great future. It has some promising real applications to the real world.

We certainly cannot say up to what extent these visions will hold true. There are some vigorous disruptions in the field of quantum computing, it will help deepen our understanding of nature and how it computes information. In the presented thesis on Quantum computers, we have explained the idea behind quantum computing and how it is different from classical computing fundamentally. Then we tried to explain the Quantum computers with respect to probability and mathematics behind the qubit based on the research from literature review provided earlier. Quantum cryptography and its advantage over conventional cryptography are explained in detail with concepts like cryptanalysis which can help immensely when quantum cryptography is accepted completely. Problem statement of the thesis is stated. Concepts behind Quantum computing, quantum physics and its drawback for wide public use is explained briefly. Theory and practical results have been shared of the experiment on IBM Q. In the later part of the report we have discussed large amount of quantum computing application such as drug development, machine learning, robotics etc. and how it can be implemented in an industry which has not accepted it yet.

Later part of the report discusses D-Wave's announcement of making a quantum computer that will out power all other classical computers. Current affairs of world have been also mentioned in the thesis, how quantum computers can help fight against COVID-19 pandemic and how some world-renowned universities are using Quantum computers to fight Coronavirus. The limitations of Quantum computing are explained such as decoherence, No- cloning theorem and complexity of hardware. In the last we explained how all the companies are working towards the goal and some recent achievements, alternative approach and methodology used to write the thesis. Ending with the conclusion we provided result to the experiment conducted on IBM Q and some future broad applications of Quantum computing.

INTRODUCTION:

Earlier in 1960's, when the first computer was designed it used to take space of a room and a number of scientists were needed to operate the machine. At that time who would have thought that 50 years later, a machine that fits on a palm can do similar amount of work. Semiconductors (which are also the replacement of switches and clicks of the original "Turing Machine") which are the building block of classical computers, it has reached the end of its contribution to the technology. Today semiconductors have become very small in macro level that there is not enough room for neither processing nor scalability of circuits which perform actions computer to further process and display results. (Bennett, Bessette et al. 1992)

Due to the sudden surge in data, classical computing system has become weak in terms of processing. The way classical computing works is that to find a solution, we give inputs to the system. If we don't provide the inputs, the classical computing fails to give a solution. At present, we are standing at a bottleneck, that means currently we have huge amount of data and incoming every second and we don't know how to deal correctly and efficiently with that data. To better utilize the data, computer needs to find a solution of the problem by backtracking the question. In this way Quantum computer can solve problems to save humankind such as global warming or how to use our resources available on earth smartly or give an alternative. (Bennett, Bessette et al. 1992)

The technology which can help us is "Quantum Computing", it is at its edge to help with more power to computation and communication. The fundamental block of quantum computing is different to classical computers. Quantum computing is a type of processing information which uses quantum mechanic's principles like quantum entanglement and superposition. Quantum computers are different to classical computers, as classical computers use 0 and 1 bits to transmit data from sender to receiver whereas quantum computers use q-bits for transmission of data. Quantum computers work on the phenomenon called superposition. In a superposition, a single qubit exhibits both the states of 0 and 1 based on probability. In practical, this qubit is a superconducting particle kept in an isolated environment free from decoherence at absolute zero temperature. This isolated particle can be an electron or photon of some selected elements which exhibit superconductivity, in which its spin decides the probability of 0's (spin up) and 1's (spin down) (Barabasi, Tappert et al. 2019).

Mathematically, a qubit is a vector representing probabilities of 0 and 1 with the help of magnitude coefficient α and β respectively which are restricted to constitute a probability of 1 i.e. α^2+ β^2=1. If α reaches to 1 then β will tend to 0.

The following equation gives an idea how a qubit works mathematically:

$$\text{Qubit } Q = |\alpha|0 + |\beta|1$$

The values of coefficients depend on the complex numbers which are real numbers that makes coefficients real as well. If either α or β reaches to 1, other must be 0 (Barabasi, Tappert et al. 2019). Let us imagine a labyrinth to explain the difference between classical computers (N^2) and Quantum computers (2^n). In a labyrinth or puzzle, a classical computer will start the solution from start if it hits a dead end or a wall whereas in a Quantum computer, properties of qubit helps in continuing the calculation for the solution.

The Literature review on Quantum Leap explains the idea of quantum computing and what difficulties it takes to achieve. Later the literature discusses the research in progress behind quantum computing and its prowess. We have also mentioned the strength, weaknesses and how to overcome the weaknesses. At the end of the literature, method and methodologies are explained followed by conclusion. The aim of this literature review is to discuss history of quantum computing with facts, focus on the questions and challenges such as scalability and financial aspect. The report also explains possibilities of future application, quantum supremacy, announcement made by companies related to quantum supremacy and recent achievements (Bernstein 2009).

Quantum computing is a type of computing which uses quantum mechanics like quantum entanglement and superposition. Usually quantum processors perform quantum computing. Quantum computers are different to classical computers, classical computers use 0 and 1 bits to transmit data from sender to receiver whereas quantum computers use q-bits for transmission of data (Bernstein 2009).

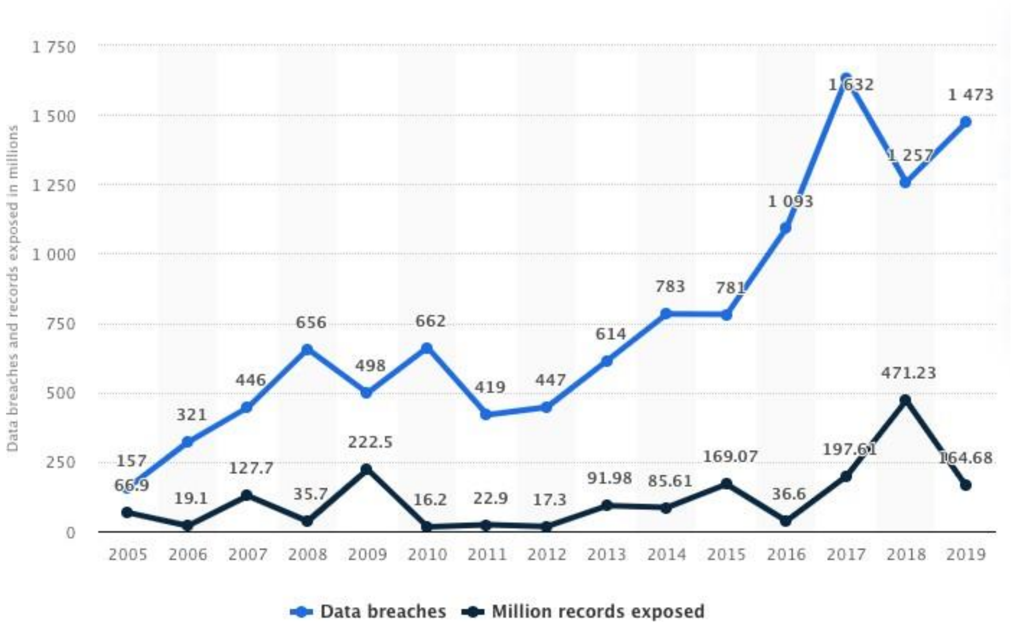
Background of Research Area:

Still as of 2020 development of quantum computers is still in its infant stages. IBM has developed a small 20 q-bit quantum computer which can be accessed online, IBM is working to release a 53 q-bit quantum computer soon. Quantum computers can solve problems more efficiently and quickly compared to a classical computer. It offers huge amount of processing power to solve problems such as factorization problems, optimization problems which classical computers cannot solve. (Bernstein 2009)

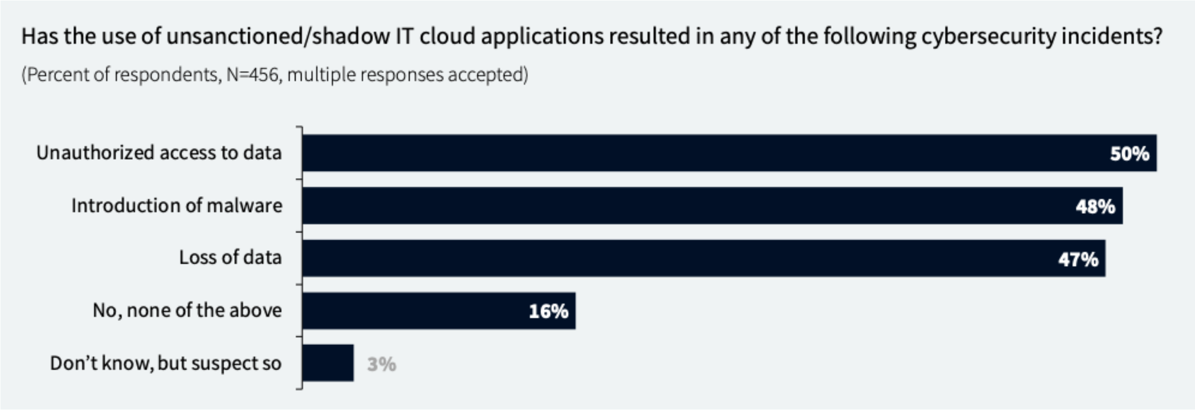
Quantum Mechanics or Quantum Physics laws guide the manipulation of data in Quantum Computers. A quantum computer is the most powerful and also hard to build computer, which can manage around 100,000 qubits. We can use it for machine learning, cryptography, and also in drug development and also in understanding the structure of molecules and also to learn and generate complex structure of chemical substances. Also universal quantum computer will be exponentially faster than a classical computer(Singh and Singh 2016).

Why Cryptography?

Majority of the security breaches occurred due to unauthorized data accessing. As per the research data till March 2020, 832 million records have been breached. As per the report published by cybint solution 62 % of the businesses experience phishing and social engineering attacks. Data breach has been increased by 67% since 2014 which is 2/3 growth of the total data breach in last 5 years since existence of data. (Kamra and Scott 2019)



The increased in data breach simply because of the technical advancement of intruders. It helped them to exploit network vulnerability by created some powerful software which enables automate attacks. In most cases the organizations are unaware about the data breach.

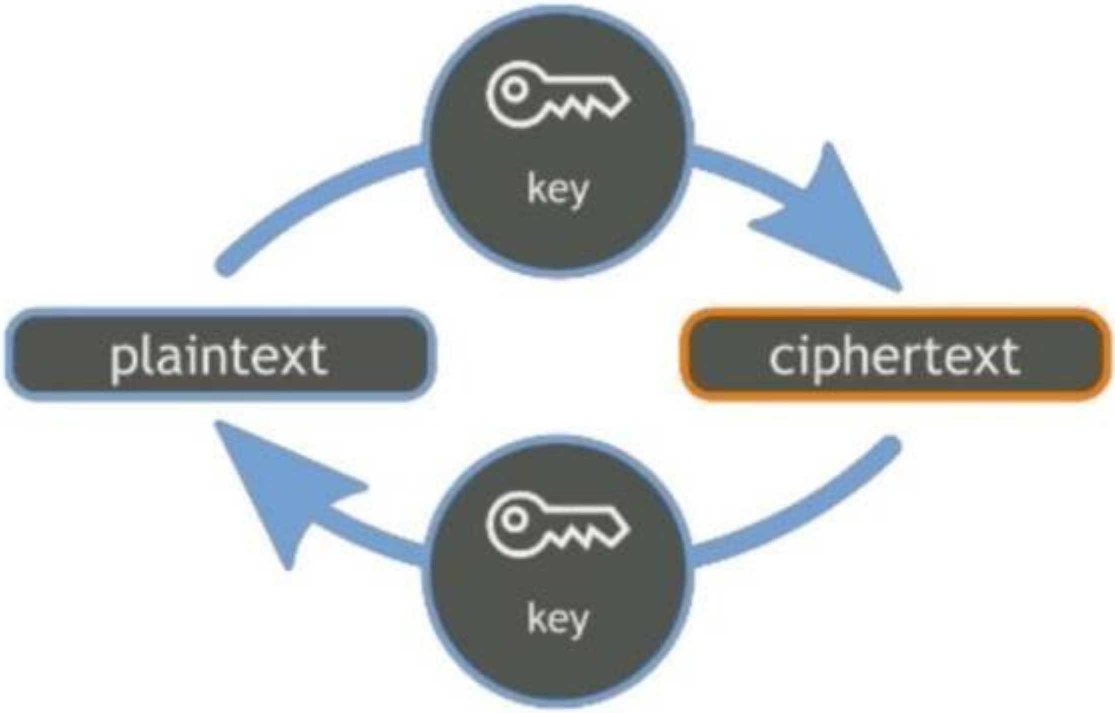


According to the security survey over 75% of the respondent lost money due to these attacks. Due to this reason cryptography is introduces to ensure a secure communication between networks. Its helps businesses to protect everything from email to bank transaction or even social media data or online shopping. (Ekert 1991)

Classical Cryptography

Cryptography is the field of science which helps us to establish a secure connection between the sender and receiver without third party intervention. Data integrity, authentication, nonrepudiation and data confidentiality are some basic tools of modern cryptography. Use case of modern cryptography or classical cryptography are Ecommerce, Automated teller machines (ATMs), computer passwords and in many other important applications. (Ekert 1991)

Classical cryptography is basically converting the plain text into some codes text using various machine learning algorithm. The keys which use to decrypt the data are shared between the sender and receiver so that they can encrypt or decrypt the message.



Classical cryptography is of two types:

1. Symmetrical cryptography– It's the least complex cryptography method in which keys used for encryption and decryption are same (Gruska 1999)
2. Asymmetrical cryptography – Its' bit complex type of cryptography method which use different keys for encryption and decryption keys are different. Asymmetric cryptography model never exchanged the private keys between the sender and receiver and it only use public keys. In this way its less prone to cyber-attacks and allows user to safely communicate data. Symmetrical cryptography– It's the least complex cryptography method in which keys used for encryption and decryption are same (Gruska 1999)

Even after all these cryptography techniques, the number of data breaches are increasing exponentially, and this data has limited computational ability which shows its incapability to deal with big data. As we are in digital era, where the volume and variety of data is out of computational limits.

Basic working principle of cryptographic algorithms developed around mathematical models and due to this reason, these models are suffering from many security defects, such as: a brute force attack, factorization problem, and many others. Thus, Due to advancement in technology the classical cryptography is not seems to be a safe option for data privacy and security. This is the reason we are moving towards an emerging technology called Quantum cryptography. (Gruska 1999)

QUANTUM CRYPTOGRAPHY:

Quantum cryptography is based on the phenomena of quantum physics which allows secure data transmission between sender and receiver. Quantum cryptography constitutes a revolution in the field of network security. (Gisin, Ribordy et al. 2002)

Quantum cryptography is a latest and advanced branch of cryptography its basis lays in the two beliefs of quantum technicalities: Heisenberg's uncertainty principle and principle of photon polarization. (Gisin, Ribordy et al. 2002)

Heisenberg's uncertainty principle says that some pairs of physical properties are related in a way that while measuring one property may prevent the person from knowing the other simultaneously. In particular, the selection of what direction to measure affects all successive measurements. When an unpolarized light enters a vertically aligned filter, it absorbs some of the light and polarizes the rest in the vertical direction. A subsequent filter tilted at some angle q absorbs some of the polarized light and transmits the rest, giving it a new polarization. A pair of orthogonal polarization states used to express the polarization of photons, such as horizontal/vertical, is referred to as a basis. (Häffner, Roos et al. 2008)

In 1984, a quantum key distribution protocol called BB84 was developed. The BB84 protocol proceeds through the following steps:

1. Sender sends polarized photons to the receiver which could be rectilinear or in diagonal direction
2. The receiver then checks for the direction of the photons by randomly selecting the basis (rectilinear/diagonal) and saves the results. Basis selected for measurement by the sender and the receiver need not be the same.
3. Through public channel the receiver informs the sender his basis of measurement.
4. Sender then sends the correct bits (bits whose basis are same) over public channel after comparing the actual basis with the received basis. The incorrect bits are discarded by the sender and receiver and the correct ones are taken as key. If an attacker uses the same basis as that of the sender the he will be able to predict the original information and if not the by this activity of the attacker the information sent is affected and because of which the receiver will either get the hampered data or no data, in both the cases the presence of attacker is detected. (Häffner, Roos et al. 2008)

Quantum key Distribution:

Key Distribution is a way of distributing encrypted keys between two parties. The simple way of key distribution is by meeting in person in a secure environment and exchanging keys. But now a days we can exchange at any distance by using Public keys like ciphers, RSA, Diffie-hellman and ecc to exchange keys (GUANCO 2015).

The problems with the conventional key distribution is that they use simple mathematical calculations to transfer data these are easy to compute and can be accessed by third parties easily (GUANCO 2015).

This classic key distribution approach has many challenges.
They are like the classic key can only generate weak random numbers which can be obtained easily by third parties. Also, the CPU power, and these keys are vulnerable to new attack strategies as they need to be re programmed again if any new attack strategies were used. Quantum computers can make these classical encryption strategies unsafe as quantum computers can decode data present in classical keys easily if quantum computers become a reality. So, to stay ahead we need to use large Asymmetric keys to securely store and distribute our symmetric keys. All these things make us to rethink the security of cryptographic keys(GUANCO 2015).
QKD addresses these problems faced by cryptographic keys by using all the quantum mechanics to transfer data or information from one point to another point(GUANCO 2015) The QKD uses a quantum channel of its own to transfer data from transmitter to receiver. It also needs a public Communication link so that it can access post processing. It also has a portal which calculates the amount of data lost through interception(GUANCO 2015)

Application (Key related work)

Quantum computing has many applications which makes it extremely powerful and useful. Some of the quantum computing application are:

- **Medical Imaging and Cure**: The most important of quantum computation is medical imaging. The combination of machine learning, artificial intelligence and quantum computing we will be able to fight a disease. Through quantum MRI machines, the physicians will be able interpret the results more efficiently due to the molecular level of the testing. With the help of machine learning trained with previous data, physicians and doctors can detect whether the patient is normal or not. Lastly by applying artificial intelligence, the disease like cancer and other deadly diseases can be cured by directly target the area without damaging other molecules of the body (Solenov, Brieler et al. 2018).
  In cancer treatment, currently computers are used to deal with thousands of variables to develop a plan for radiation that can directly affect the cancer cells leaving other healthy cells undamaged. The power of quantum computing can result in ideal radiation dose at the targeted cell without any side effects (Solenov, Brieler et al. 2018).

- **Machine learning**: Machine learning can be completely defined under three categories i.e. Supervised, unsupervised and reinforced machine learning. All the three kinds of learning involve huge computing power. Some of the examples are:
  1) Support Vector Machine (SVM): SVM uses brute force algorithm on a classical computer which involves great processing power and time. Quantum algorithm such as Grover's search algorithm provides speed up to the process.

  2) K- nearest neighbor algorithm (KNN): KNN is a classification algorithm which classifies object into clusters i.e. group of points based on same features. As the number of clusters increases to classify complexity also increases for a classical computer. This type of tasks can be better handled in a quantum computer where it offers parallel computation. It can compute object's distance from the cluster's centers simultaneously.

3) Perceptron: The main objective of perceptron is to find a hyperplane which fits the training data well, it creates number of possibilities of hyperplanes that makes classical computer slow as it is calculating all the points to a single hyperplane simultaneously. Whereas what Quantum computers can offer is results of multiple hyperplanes to the points.

There are theoretical proofs that quantum computing offers quadratic speed up over classical computing (Ablayev, Ablayev et al. 2019).

- **Application of 6G or B5G**: With the advent of 5G, there has been speculations that in a decade 5G technology will fail to satisfy the data need. Plan with framework is presented in (Nawaz, Sharma et al. 2019). It explains that with the help of artificial intelligence (AI) and Machine Learning (ML), the idea of automatic switches and self-serviceable network can provide 100 times more data speed compared to 5G network will provide. By 2030, it is estimated that growing traffic will generate approximately 5,016 exabytes of data every month. Both the components ML and AI need parallel processing to deliver results and service networks in real time. Quantum computers offers ML and AI unparalleled parallel computing which will meet the rapid increase in demand of fast, reliable, secure, intelligent and green internet (Nawaz, Sharma et al. 2019).
- **Cryptography:** Big Data is a cluster of data sets with sizes beyond the capacity of commonly used software tools like database management tools or conventional data processing applications to capture, curate, handle and study in realistic time. With the entrance of big data arises the hazard of advanced security violations as data volume enlarges**.** Implementation of big data security should include two things, Firstly, secure encryption technology must be used to protect confidential data. Secondly, careful management of access to cryptographic keys which unlock the encrypted data must be put in place. Artificial neural network is an information processing model taken from biology where neural network have an important task in human body. The key module of this structure is its information processing system. It is a collection of large number of highly organized processing elements operational in unity to solve particular problems.

- **Optimization and language problem for robotics**: The power Quantum computing offers is very important in the field of robotics. Modern day robots require fast image processing to access the information of the surrounding. Real time image processing requires huge processing power which becomes very expensive for classical computing. With the help of entanglement, superposition and quantum algorithms robots will be able to store, process and secure efficiently. The basic idea is that different colors can be encoded in the particle’s spin(Petschnigg, Brandstötter et al. 2019). Different information can be stored in the different position of particle which will allow the robot to have random access to almost infinite memory.

- **Privacy and Security** – Quantum uncertainty can be useful in order to generate private keys for encrypting messages. We can float these encrypted messages from one location to other without having a fear of decoded by any unreliable source because of the quantum uncertainty. To break these keys and pull out the information from these messages which is next to impossible. Banks and other financial institutions are already started using these unbreakable encryption.(Steane 1998)

- **Drug Development** – Quantum technologies are very helpful in transforming medicines and health care. For example – the most challenging problem for drug development is analysis and designing of a molecule. Quantum technology can calculate the quantum properties of all the atoms which is computationally a difficult task even for a powerful super computer. Quantum computing use quantum properties to simulate a molecule which gives it's an advantage over classical technology. Treatment of disease like Alzheimer can be effectively executed due to large scale quantum simulation. (Leuenberger and Loss 2001)

- **Information Teleportation**- An interesting feature of quantum technologies is information transfer from one place to another without physically transmitting it. It can be possible due to fluid identities of quantum particles which can get entangled across space and time in such a way when we change something in one particle it's has an impact on other particle and it creates a channel for teleportation. (O'brien 2007)

Problem Statement:

The biggest challenge stands against quantum industry is to bring quantum computers or its various applications to commercial and wide use despite of its limitations. The main aim is to bring quantum computers is to solve unsolved questions which we have been not able to solve.

CRYPTANALYSIS:

Quantum cryptanalysis is understanding the meaning of the encrypted information by not accessing the original information. In this we try and find the secrete key.(Ma 2008). We also study the attacks to get the encrypted information. This study of attacks can be done by investigating the security in a practical way. In general the practical problem in a QKD system is the detection of loop holes by using Cryptanalysis we can study those loopholes(Ma 2008).

Entanglement:

Electrons or Qubits if they are interacted at any point will have a connection in between those particles. If any electrons or Qubits show these features, then they are called as they are in correlation or they are entangled together. After knowing the spin of one electron the other entangled electron will have its spin in the opposite direction to the other electron. Because of the use of quantum superposition, the particles have no spin or direction before calculations, but the particle exists alternatively in both up and down or in 0s and 1s states. The spin of a particle is measured at the time of measurement and it simultaneously communicates to its entangled particle, it possesses opposite spin direction to that of the original spin of the measured particle. With this property the qubits can interact No matter how great the distance between the mutually related particles, they will remain entangled as long as they are isolated. (Jennewein, Simon et al. 2000)

Quantum teleportation:

Quantum states are highly unstable, if they interact or collide with any other systems then it will lead in either losing their superposition properties or even destroying. If any errors occur with classical bits they can be resolved easily when compared to that of Quantum bits. Quantum teleportation focuses on transferring of information by using unknown quantum states and through a protected environment. If in future this application becomes a reality we can transfer outputs generated by a computer can be used as inputs by teleporting outputs(Spiller 1996). Teleportation uses the property of quantum entanglement. It helps in the transfer of information from one point to another point. Free space quantum communication is a reality as communication can be done for almost 200kms through links. It was proved practically (Spiller 1996).

Applications of quantum cryptography in Cyber Security:

The advantages present in the quantum computers will make the public keys like RSA, Ellamae and other public keys will no longer be safer in the quantum computers. Also, problems like Discrete logarithm problem or integer factorization can be easily solved using quantum computers. So in order to secure these systems we need different cryptosystems which are not based on the above problems. (Zhou, Shen et al. 2018)

Both network security and Cryptography are key in ensuring the safe security of the information systems. One of the main essentials of Cyber security is to explore the quantum cryptographic protocols. (Zhou, Shen et al. 2018).

Quantum information has some of the unique properties which classical information doesn’t possess. Mainly information of quantum codes present in entangled state is hard to obtain.(Zhou, Shen et al. 2018)

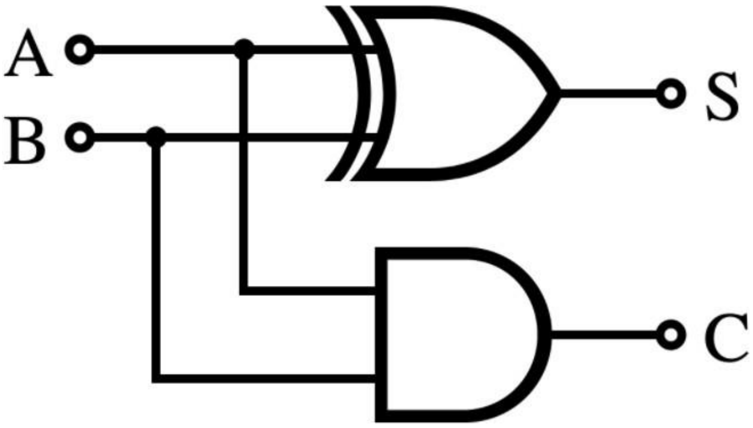
1. Uncertainty principle: This principle states that the position of a particle in the Micro world is hard to determined and also it states that the particles position is different in different places.

2. Quantum No-cloning: Cloning is Producing an identical quantum particle in a complete different state. It has been proved by the scientists that the Quantum machines can reflect this property. Quantum states also have a feature called as the undeleting property. This means deleting or damaging of a particle in quantum states will leave a trace in Communication systems. Deleting a copy of a quantum state is not allowed by linearity of quantum mechanics(Zhou, Shen et al. 2018).

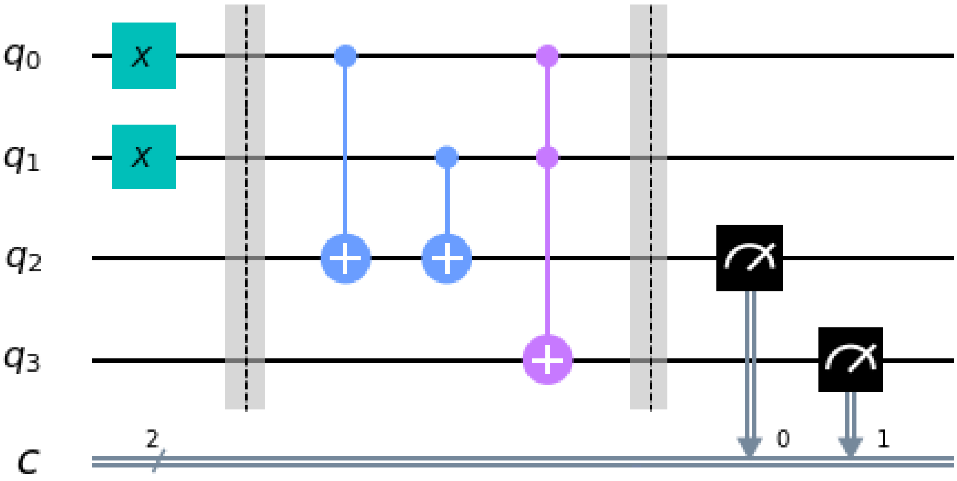
Quantum Circuits:

It is a computational practice which involve coherent quantum operations on quantum data, commonly known as qubits, and coexisting real-time classical computation. It is a sequential arrangement of quantum gates, measurements and resets.(Politi, Cryan et al. 2008)

It all starts from basic representation, below is an classic circuit diagram with logical AND, OR gates are used, where inputs are at the left side of the circuit and output is at the right side of the circuit:



The quantum circuit of the same logical circuit diagram can be represented as below:

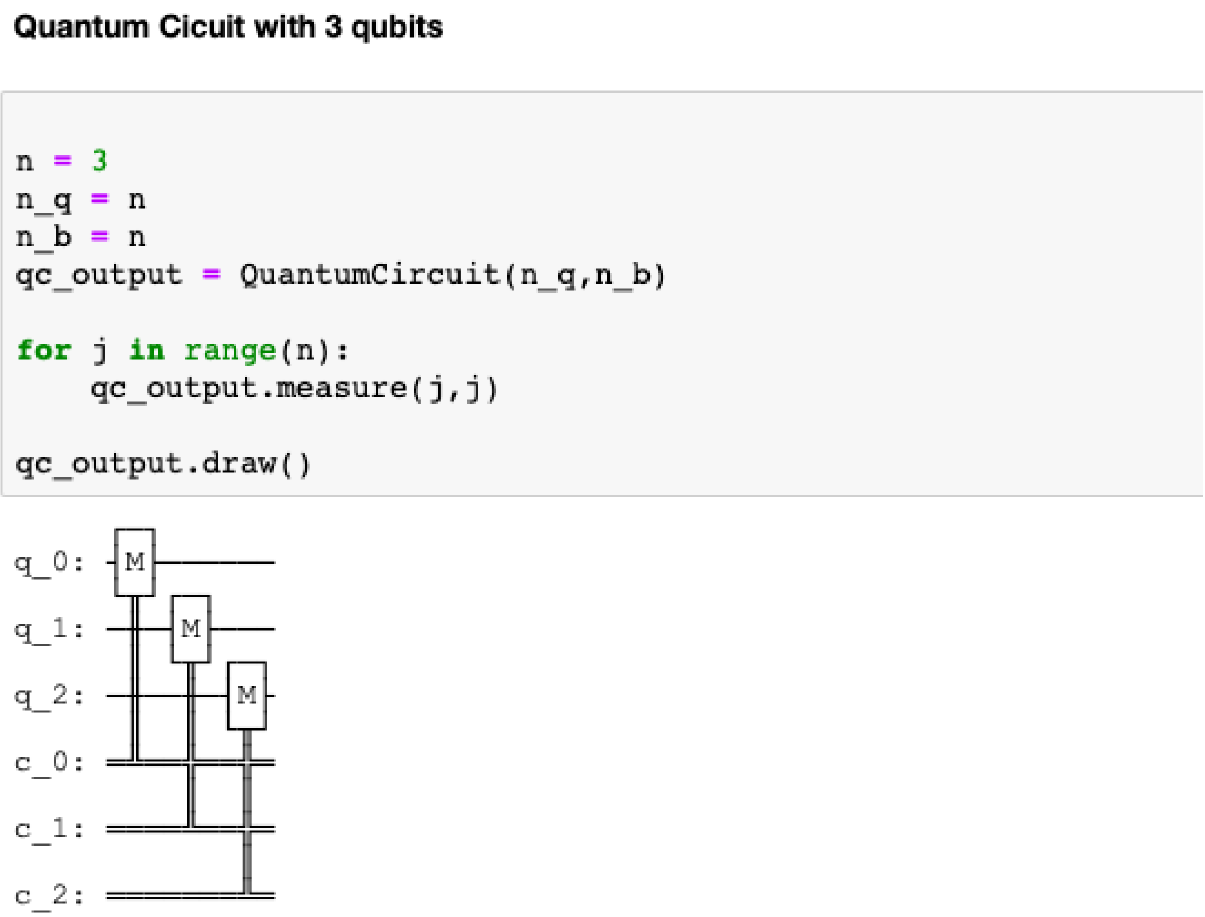


(Gu, Kockum et al. 2017)

To build a quantum circuit, we just need to follow three steps:

1. Encode the inputs
2. Apply logical computation
3. Extract the output (Politi, Cryan et al. 2008)

We can make quantum circuit with any number of qubits, We have used 3 qubits to demonstrate a quantum circuit



Quantum Cicuit with 3 qubits

```
n = 3
n_q = n
n_b = n
qc_output = QuantumCircuit(n_q,n_b)

for j in range(n):
    qc_output.measure(j,j)

qc_output.draw()
```

(Xiang, Ashhab et al. 2013)

Qubit Gates: Single Qubit Gates
We can represent the qubits by 2D vectors, and that their states are limited to the form:

|□⟩ =cos(□2) |0⟩ +□□□sin□2|1⟩

Where θ and ϕ are real numbers.

We will be going to discuss about the various logic gates operations and the qubit orientation. Due to the similarities between the gates there might be a risk of becoming of list.

The Pauli Gates

Pauli gates matrix are based on the basic linear algebra principles. It is used to represent some of the very common quantum gates.

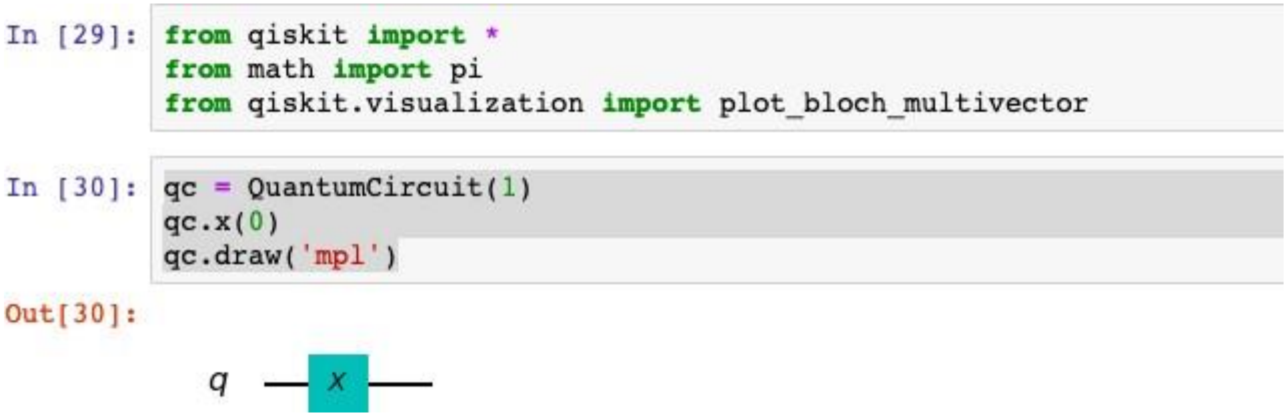
1.1 The X-Gate

Pauli-X matrix representation of X gates is shown below:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

We can simply evaluate the effect of a gate by just multiplying the qubit's state vector by the gate. It is clearly indicated that the X-gate switches the amplitudes of the states $|0\rangle$ and $|1\rangle$:

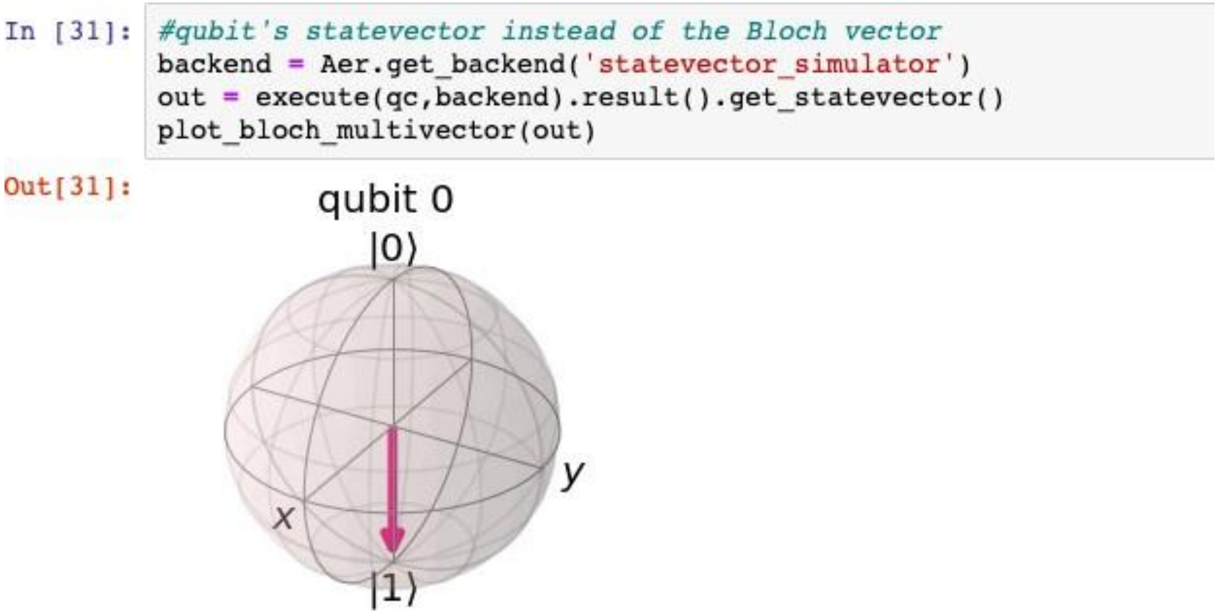
$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$



```
In [29]: from qiskit import *
         from math import pi
         from qiskit.visualization import plot_bloch_multivector

In [30]: qc = QuantumCircuit(1)
         qc.x(0)
         qc.draw('mpl')

Out[30]:
```

(Politi, Cryan et al. 2008)

We can even visualise the actual state representation of qubit's state vector by using the plot_bloch_multivector() function.



```
In [31]: #qubit's statevector instead of the Bloch vector
         backend = Aer.get_backend('statevector_simulator')
         out = execute(qc,backend).result().get_statevector()
         plot_bloch_multivector(out)
```

Out[31]:

(Barends, Kelly et al. 2014)

<u>Problem Statement</u>:

Suppose there are 2 scientist Alice and Bob. Alice and Bob both are research scientist and working the healthcare industry from last 30 years. Alice is from United states and Bob is from Australia. They are working on COVID -19 Vaccine and whatever the research work they are doing; they just want to protect it from unauthorised user (Say Eve) who might misuse the data. The aim is to safely communicate the data between these two without any data breach.

We will be going to solve this problem by making sure the communicated data between the sender and receiver is always safe and make sure that any unauthorised user cannot access the data. This is possible by using Quantum Key Distribution (QKD).

Quantum Key Distribution is a branch of quantum cryptography which ensure the safe data transmission between two parties, a sender, Alice and a receiver, Bob. Classical cryptography techniques are based on the key distribution that rely on unproven computational assumptions whereas QKD follows the phenomena of quantum mechanics. In classical cryptography is simply reliable on the eavesdropper computation capabilities. In these techniques they can only hope that an unauthorised user does not have a very high computational resources to access the information in transit.(Lo, Ma et al. 2005)

Quantum Key Distribution is a technique, which is based on phenomena of quantum physics instead of classical cryptography which is simple based on computational complexity of mathematical problems, which generate and distributed the complicated cipher keys on a unsecure communication channel where any one can attack and access that valuable information. Quantum key distribution is based on using the single photon technology that can detect any potential unauthorised access on the data via quantum bit error rates of the quantum channel which we are going to demonstrated in this section later.

A QKD system basically involved two type of channels which is classical channel and quantum channel. The classical channel can be treated as traditional IP channel (which may or may not be optical). It entirely depends on the system design and it might be closely attach and devoted to quantum channel which will use it in timing requirements. Quantum channel is a lossy and probabilistic channel which is mainly used to transmit the Qubits (single photons) and it consist of optical path which must be transparent.(Gottesman, Lo et al. 2004)

Quantum Key Distribution Protocols are used to provide sharing unique keys between sender and receiver on communication channel. A secure communication can be possible by using these unique keys even on an insecure public network. Mostly the poorly designed key distribution protocols suffer from security problems. Hence, key distribution protocol designing is the utmost priority in a communication system. In some key distribution protocols, a Trusted Centre (TC) is involve which pass the keys to sender and receiver. These protocols which involve three party's sender, receiver and TC are called three party distribution protocols. It is considered to be a better protocol than the usual two party protocol where there is key negotiations happens between only two parties.(Shor and Preskill 2000)

In classical cryptography, to prevent replay attacks three party key distribution protocols are used which effectively use timestamp to figure out the replay attacks. However this approach is not solid proof, it is based on the assumption of clock synchronization which is almost impossible in distributed systems due to hostile attacks and unpredictable nature of network delays. This is the reason why classical cryptography is not able to detect passive attacks which is commonly known as eavesdropping.(Scarani, Bechmann-Pasquinucci et al. 2009)

The major difference between the quantum cryptography and classical cryptography is that the quantum key distribution protocols (QKDPs) utilize quantum mechanics to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key. There are some additional communications rounds required between sender and receiver in the case of public discussion whereas in classical cryptographic approach has more efficient techniques for key verification and user authentications.(Goyal, Aggarwal et al. 2011)

There are two three-party Quantum Key Distribution Protocols, one with verifiable client validation and the other one with unequivocal common authentication, are joined to show the benefits of consolidating both old style and quantum cryptography. Likewise, when contrasted and Classical three-party key dissemination conventions, the proposed QKDPs effectively oppose replay assaults. This work presents another course in structuring QKDPs by consolidating the benefits of Classical with quantum cryptography. (Wasankar and Soni 2013)

There are not many quantum key appropriation conventions depicted in, for example, BB84 quantum cryptographic convention, B92 quantum cryptographic convention, Entanglement-based quantum key dissemination and Quantum Bit Commitment (QBC) conventions. Likewise this paper incorporates convention assessing and examination, utilizing such measures as blunder probability, quantum and old style memory limits, commotion affectability. (Lo and Chau 1997)

A portion of the upsides of Quantum Cryptography over old style cryptography portrayed in i.e., it gives us entirely secure information transmission. Additionally, it talks about Quantum Key Distribution and how significant quantum cryptographic conventions are to it. It additionally tells about how listening in can't avoid being in quantum cryptography and its belongings.

The security of a portion of the quantum cryptographic conventions, for example, BB84 convention, Six- state convention, SARG04 convention, Symmetric and Asymmetric three-state convention. The creators likewise analyse their exhibitions in both the perfect case and a sensible case and found that Efficient BB84 and Six-state conventions endure the most elevated QBER.

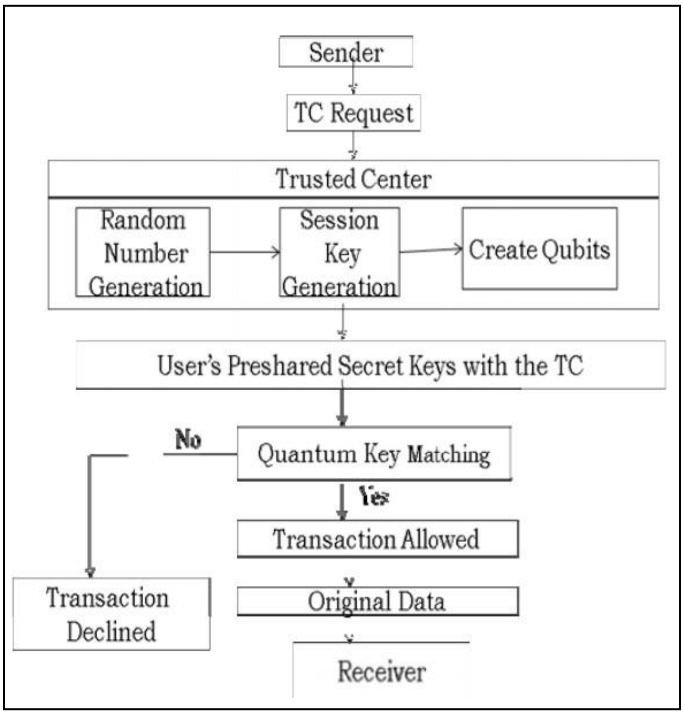


Fig: System Architecture

As appeared in Figure, in the proposed QKDPs, the TC and a member synchronize their polarization bases as per a preshared mystery key. During the meeting key appropriation, the preshared mystery key along with an arbitrary string are utilized to deliver another key encryption key to encipher the meeting key. A beneficiary won't get a similar polarization qubit regardless of whether an indistinguishable meeting key is retransmitted.

Quantum Key Distribution Protocols Implementation

In 1984, Bennett and Brassard planned a convention (creatively named the BB84 convention) dependent on the above conduct utilizing four polarization expresses that fills in as follows: The sender encodes the data into quantum states utilizing an irregular arrangement of bases and transmits the data to the collector. Each piece of this information will be as a short eruption of light, energized utilizing the said bases of estimation. The beneficiary at that point peruses the approaching data utilizing their own arbitrary arrangement of bases. When the information has been moved, it just stays for the sender and collector to openly talk about which bases were utilized and in which request. At whatever point the bases concur, it very well may be demonstrated that the pertinent piece of data is indistinguishable at the two parts of the bargains, with the exception of in the accompanying two circumstances: (Grosshans, Van Assche et al. 2003)

a) When arbitrary commotion disturbs the information channel.

b) When an eavesdropper attempt to catch the information stream.

For the recreation, every one of item (Alice, Bob, Eve, Quantum Channel, Public Channel) assume distinctive job. Just the fitting capacity is executed in every one of workstation, relies upon its job. The convention fills in as follows:

1. Alice produced a length (k) of arbitrary number (0 and 1), at that point sends it on quantum channel to be perused by Bob and Eve.

2. In the event that there is listening stealthily from Eve, Eve is the person who need to peruse the quantum channel object first. Eve can change the bits with two sorts of assaults: capture/resend or shaft parting.

3. At that point, Bob peruses the refreshed form from quantum channel object, accepting that Bob doesn't think about the tapping from Eve.

4. Bounce at that point quantifies the bits he read from quantum channel object with his chose own bases. At that point Bob declares the bases he made to Alice by means of open channel, which situated at Alice's.

5. Filtering crude key start, Alice read Bob's estimation at open channel protest and affirm to Bob the position Bob has gauges in the correct bases (m bits) by declaring it at open channel.

6. Next, Alice and Bob gauge mistake to distinguish spy. The two of them compute and look at their bit mistake rate (e). In the event that they found that their blunder rate is higher than greatest piece mistake rate ($e > e_{max}$), they will suspend the correspondence and start from the very beginning once more. (e_{max} has a foreordained worth)

7. Presently, both Alice and Bob will have a mutual key, which is called 'crude key'. This key isn't generally shared since Alice and Bob's form are unique. They kill the m bits from the crude key.

8. Both Alice and Bob at that point performs 'mistake amendment' on their crude key to discover mistaken bits in uncompared parts of keys and 'security intensification' to limit the quantity of bits that a spy knows in the last key.

9. At long last, the two of them will get an equivalent series of bits, which is the common mystery key. (Jennewein, Simon et al. 2000)

Quantum cryptography, or quantum key dispersion (QKD), utilizes quantum mechanics to ensure secure correspondence. It empowers two gatherings to deliver a common irregular piece string known distinctly to them, which can be utilized as a key to scramble and unscramble messages.

A significant and special property of quantum cryptography is the capacity of the two conveying clients to identify the nearness of any outsider attempting to pick up information on the key. An outsider attempting to listen stealthily on the key should somehow or another measure it, in this manner presenting discernible inconsistencies. By utilizing quantum superposition or quantum trap and transmitting data in quantum expresses, a correspondence framework can be actualized which distinguishes spying. In the event that the degree of spying is underneath a specific limit, a key can be created which is ensured as secure (i.e., the meddler has no data about), in any case no safe key is conceivable and correspondence is prematurely ended (Barrett, Hardy et al. 2005)

VI. Reproduction RESULTS

This paper is guaranteed to give the accompanying outcomes come what may:

1. Quantum Key Distribution (QKD) utilizes quantum mechanics to ensure secure correspondence.

2. Quantum Key Distribution empowers two gatherings to create a mutual key known uniquely to them, which can be utilized as a key to scramble and decode messages.

3. The capacity of the two clients to identify the nearness of any outsider who is attempting to listen stealthily the common key.

4. Verify each other after the information transmission with the assistance of meeting keys, to forestall man-in-the middle assault.

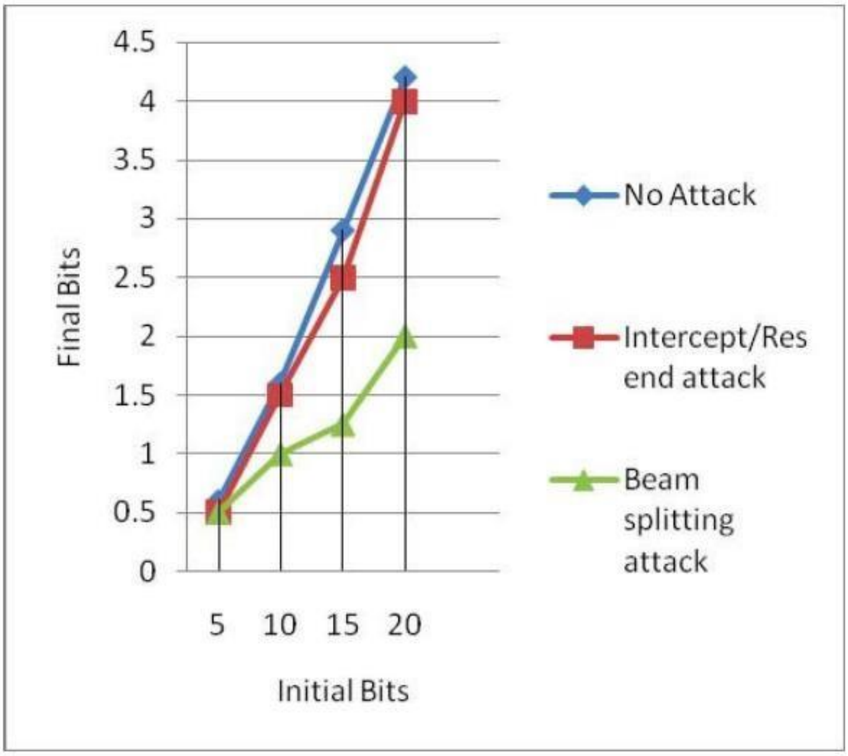


Figure: Initial vs Final Bits Length

In Figure, x-axis speaks to starting bits which its length is contribution from sender (Alice), while y-axis speaks to conclusive bits length that have been produced all through the convention. Three sorts of assaults are thought of, that incorporates no-assault, block/resend and bar parting that have been utilized inside this reproduction to look at the impact of assault presence. (Van Assche 2006)

From the Figure, we can see that regardless of whether there is no assault Bob despite everything can't increase flawless bits length send by Alice, this is on the grounds that in Quantum Channel itself, there are likewise other impact that cause to defective channel. Along these lines, there is still a little blunder on their bits during the transmission. (Renner 2008)

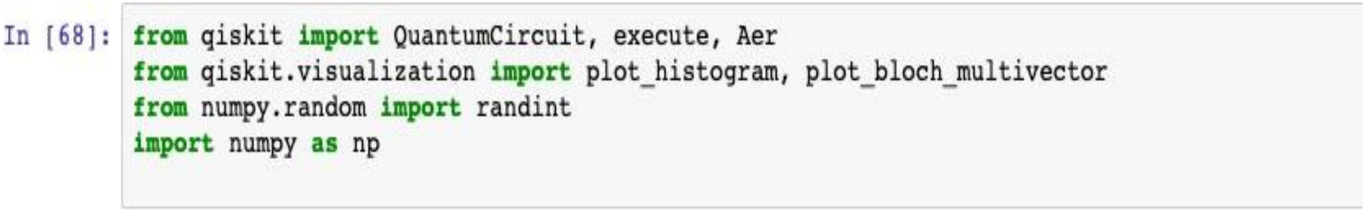
Capture/resend assault gives length of conclusive bits practically equivalent to no-assault. In block/resend assault, Eve will produce another string of arbitrary key and send it to Bob as though the key string has been send by Alice. In this way, the probabilities for Alice and Bob can distinguish Eve exist is half (expanded). The likelihood that key string that produced by Eve like Alice is half. The two of them despite everything can identify that mistake rate (e) is still lower than the most extreme blunder rate ($e < e_{max}$) and proceeded to blunder amending process. (Inamori, Lütkenhaus et al. 2007)

Number of conclusive bits length in shaft parting assault is a lot of lower than the other two assaults on the grounds that; in this assault an irregular number of Alice's bits are part by Eve. Along these lines more mistake can be distinguished by Alice and Bob in 'blunder revision' process. In spite of the fact that the mistake rate (e) is still lower than the greatest blunder rate ($e < e_{max}$), Alice and Bob can distinguish as much as half of mistake in their filtered key. The length of revised key is higher than other two assault prompts the greater part of the bits need to take out in 'mistake rectification' procedure to limit the data for Eve.

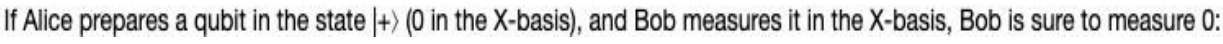
Quantum Key Distribution Protocol using Qiskit

Protocol Overview:

Basically, the aim of the QKD protocol is to identify the change in Qubit’s state. If Alice sends a qubit to Bob, and an eavesdropper (Eve) tries to measure it before Bob does, there is a very high chances that there will be a change in qubit state and



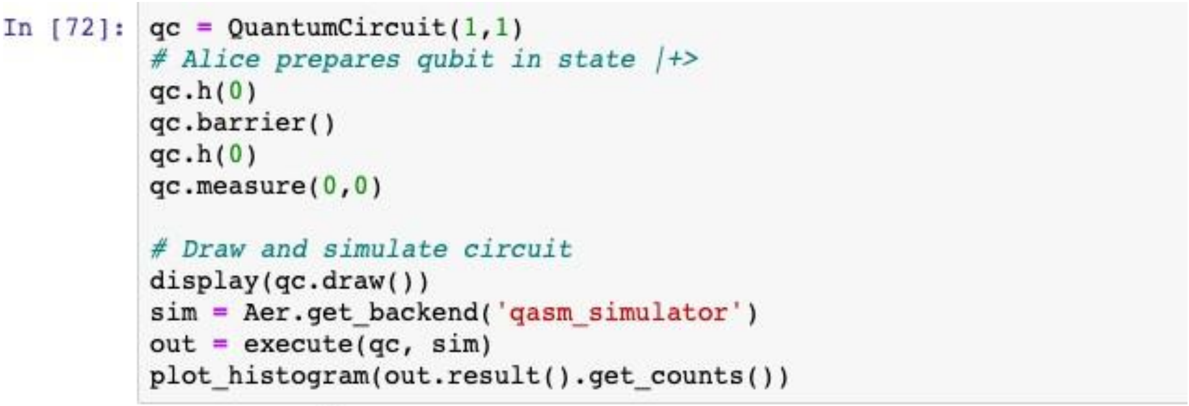
```
In [68]: from qiskit import QuantumCircuit, execute, Aer
         from qiskit.visualization import plot_histogram, plot_bloch_multivector
         from numpy.random import randint
         import numpy as np
```



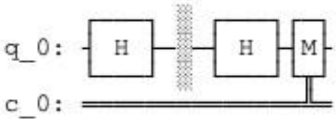
If Alice prepares a qubit in the state $|+\rangle$ (0 in the X-basis), and Bob measures it in the X-basis, Bob is sure to measure 0:

(Cross 2018)

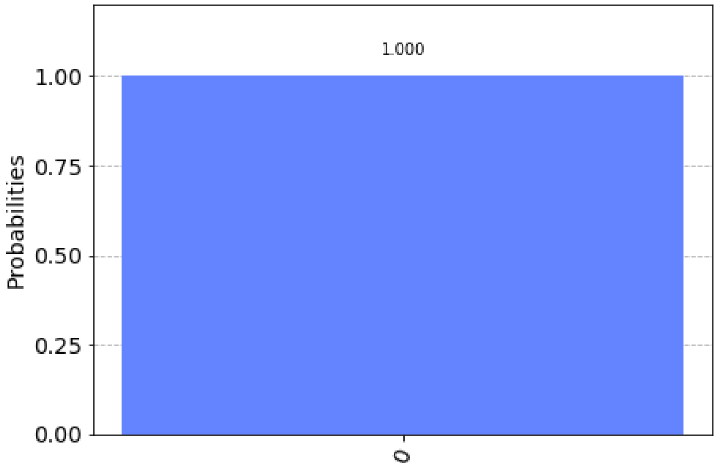
Here in 1st scenario, Alice sends qubit to Bob which measure in X axis



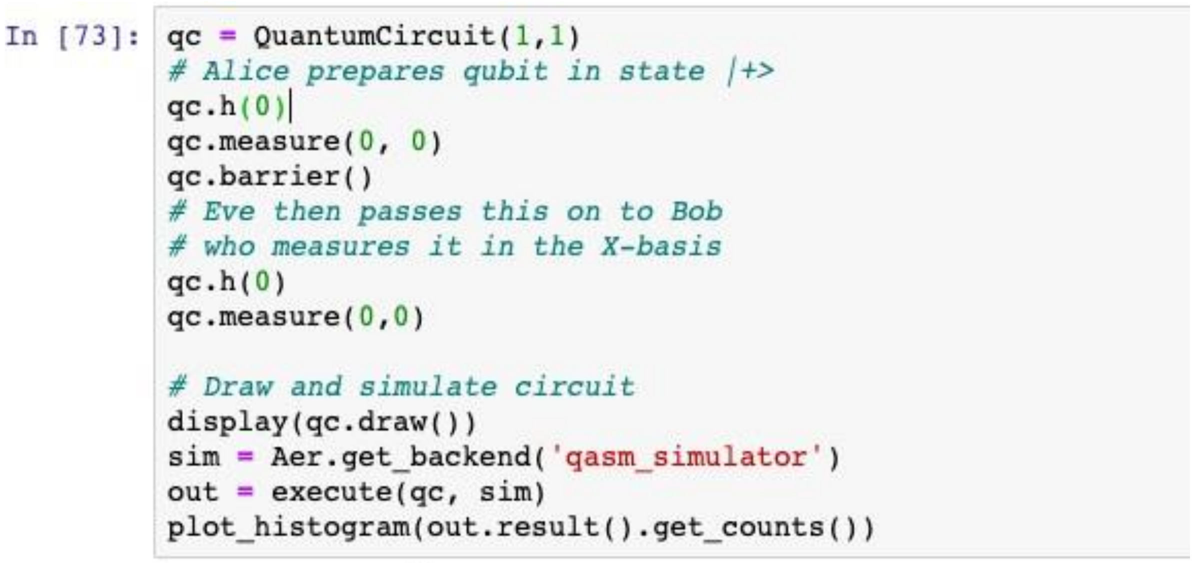
```
In [72]: qc = QuantumCircuit(1,1)
         # Alice prepares qubit in state |+>
         qc.h(0)
         qc.barrier()
         qc.h(0)
         qc.measure(0,0)

         # Draw and simulate circuit
         display(qc.draw())
         sim = Aer.get_backend('qasm_simulator')
         out = execute(qc, sim)
         plot_histogram(out.result().get_counts())
```



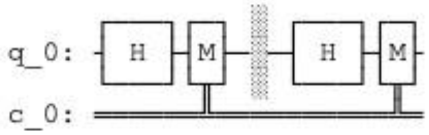
Out[72]:



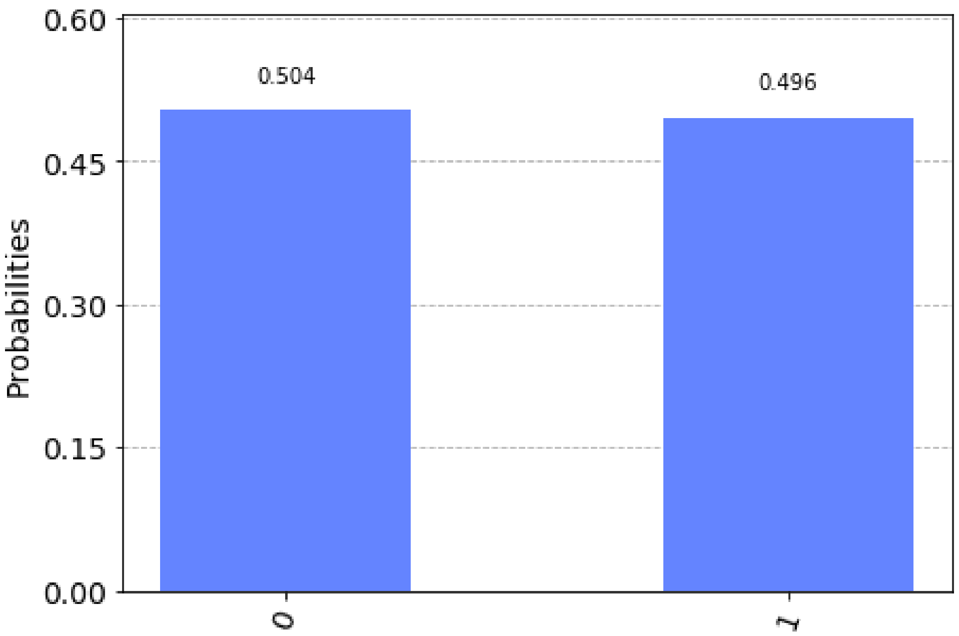
In 2nd scenario, Alice sends qubit to Bob but eve intervened and tried to read it



```
In [73]: qc = QuantumCircuit(1,1)
         # Alice prepares qubit in state |+>
         qc.h(0)
         qc.measure(0, 0)
         qc.barrier()
         # Eve then passes this on to Bob
         # who measures it in the X-basis
         qc.h(0)
         qc.measure(0,0)

         # Draw and simulate circuit
         display(qc.draw())
         sim = Aer.get_backend('qasm_simulator')
         out = execute(qc, sim)
         plot_histogram(out.result().get_counts())
```



Out[73]:



We can see here that Bob presently has a half possibility of estimating 1, and on the off chance that he does, he and Alice will know there is a major issue with their channel.

The quantum key dispersion convention includes rehashing this procedure enough occasions that a eavesdropper has an irrelevant possibility of pulling off this capture attempt. It is generally as follows:

Step I

1. Alice choses a random bit of string, e.g.:

   1000101011010100

2. Random Basis for each string will be:

   XZXZXXXZXZXXXXXX

Step II

Alice at that point encodes each piece onto a series of qubits utilizing the premise she picked, this implies each qubit is in one of the states $|0\rangle$, $|1\rangle$, $|+\rangle$ or $|-\rangle$, picked aimlessly. For this situation, the series of qubits would resemble this::

$|-\rangle$ $|0\rangle$ $|+\rangle$ $|0\rangle$ $|1\rangle$ $|0\rangle$ $|1\rangle$ $|+\rangle$ $|1\rangle$ $|-\rangle$ $|+\rangle$ $|-\rangle$ $|0\rangle$ $|-\rangle$ $|0\rangle$ $|+\rangle$

This is the message Alice send to Bob

Step III

Now Bob will do the random estimation of each qubit ,he can use any estimation . For ex:

XZZZXXXZXZXZZZXZ

Bob keeps the estimation results hidden.

Step IV

Now Sender (Alice) and receiver (Bob) share their basis publicly which they use for each qubit. They only use it use it as a secret key if they both measured the basis in the same pattern otherwise, they will discard the information.

Step V

At last, if both will share the random sample of their keys, and if the samples match, it is an indication of a successful transmission. We can use the same QKD protocol to share the covid-19 data.

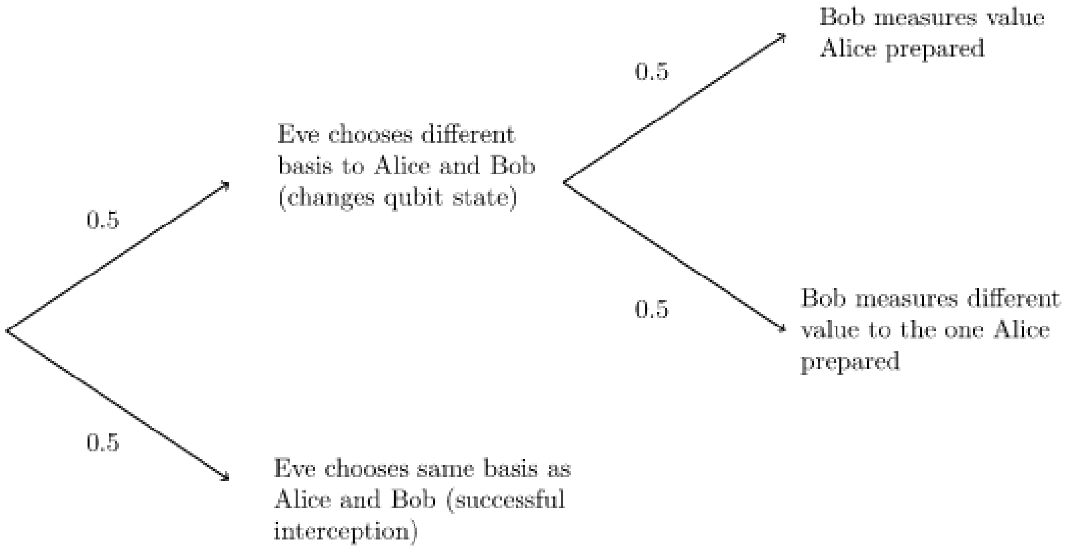
Risk Analysis

In this interception where eve measures all the qubits, there is a minute possibility that Alice and Bob’s samples could not match, and they try to send unprotected message through Eve's channel. We are estimating a vulnerability of quantum key distribution

- For Alice and Bob to utilize a qubit's outcome, the two of them probably picked a similar basis. On the off chance that Eve choses this premise as well, she will effectively block this bit without presenting any mistake. There is a 50% possibility of this incident.

- If Eve choses an inappropriate basis, for example an alternate basis to Alice and Bob, there is as yet a 50% possibility Bob will gauge the worth Alice was attempting to send. For this situation, the block attempt likewise goes undetected.

- But if Eve choses an inappropriate basis, for example an alternate basis to Alice and Bob, there is a 50% Bob won't measure the worth Alice was attempting to send, and this will introduce an error in their keys.


0.5
Eve chooses different basis to Alice and Bob (changes qubit state)
0.5
Bob measures value Alice prepared
0.5
Bob measures different value to the one Alice prepared
0.5
Eve chooses same basis as Alice and Bob (successful interception)

(Woerner and Egger 2019)

n the event that Alice and Bob look at 1 apiece from their keys, the likelihood the bits will coordinate is 0.75, and if so they won't notice Eve's capture attempt. On the off chance that they measure 2 bits, there is a 0.752=0.5625 possibility of the capture attempt being taken note. We can see that the likelihood of Eve going undetected can be determined from the quantity of bits (□) Alice and Bob decided to analyse:

▯(undetected)=0.75▯

On the off chance that we choose to look at 15 bits as we did above, there is a 1.3% possibility Eve will be undetected. On the off chance that this is unreasonably hazardous for us, we could look at 50 bits rather, and have a 0.00006% possibility of being spied upon accidentally.

It shows that the we want to share COVID -19 Sensitive data we can use high number of bits which gives us a surety of secure data transmission.

IBM Summit

Summit is a supercomputer which is Developed by IBM Technologies. It was first developed at Oak Ridge National Laboratory. At present it is the fastest Supercomputer in the world. It has a processing speed of 148.6 petaflops. It is also the first supercomputer to reach exaflop. It is predicted to reach 3.3 exaflops using various mixed precision calculations.

Now IBM is using this supercomputer to help in the battle against COVID-19. The initial use of IBM Summit is to solve complicated or impossible tasks in the field of energy, Human Health and Artificial intelligence. If Researchers use IBM Power9- systems, we can observe results in the span of -2 days which usually take months for a classical computer to perform. Researchers were provided with summit so that it will increase processing speed and reduce processing time of Simulations.

With this work researchers found somewhere around 77 Small-Molecule Drug Compounds which would further help in the study and also help in the fight against COVID-19. The Supercomputer Identified around 8000 compounds which are most likely to combine together to create a main “Spike” on the protein of the coronavirus. Another university built a similar kind of protein which also has the same “spike” Called as the S-Protein. They used some chemical simulations code to perform Molecule Simulations, Which Analyse Atoms movements inside the proteins.

Oak Ridge National Laboratory Then used various compounds to see if they can destroy the spikes of the protein which are sticking to the human cells. Summit Ranks all the compounds based on how likely they can break the Spike to unlink with the Human cell. Although these results doesn’t mean that a cure is found for deadly COVID-19 Virus, But the compounds which are active against the proteins can be useful in further studies. So, then we know if the compounds exhibit the characteristics we need to kill a virus.

Researchers used Summit’s massive data processing capacity 4608 IBM PS AC922 Nodes, each with 2 IBM power9 CPU’s, Giving it a performance of 200 petaflops. Summit is also used to understand the origins of this universe, and also if Humans can survive on the mars. For These we need to analyse Minerals and their atomic composition. (Hines 2018)

Related Work:

Quantum computers are a real thing now. A few companies offer their service via cloud, one of the examples are IBM Q. And this is only possible when the phenomenon in Quantum physics called “Entanglement” is combined with superposition. Entanglement can be defined as “Spin of one particle effects the spin of other particle”. The above statement is only true when both the particles should be in isolation (free from all kind of noise) and energy of the environment (that can only be achieved in either space or in absolute 0-degree temperature). Famous scientist Albert Einstein defined Entanglement as “Spooky action at a distance” (Einstein, Podolsky et al. 1935).

The power of quantum computing can be increased exponentially. Every qubit that is added to a quantum computer increases the processing power exponentially by 1 (if we want to double the processing power of quantum computer with 20 qubit we only have to add just 1 qubit to the system i.e. quantum computer’s processing power increases with a factor 2^n whereas classically the processing power increases with a factor of N^2). A milestone was achieved in 2019 by Google where Google conducted an experiment on a quantum processor called sycamore consisting of 54 qubit (out of which 1 qubit was not working) and reached quantum supremacy by solving a problem of factorization in 200 seconds for which a classical computer will take 10,000 years(Aaronson 2008).

Real World Applications of Quantum Computing:

The exponential development in processing power that accompanies the advancement of a feasible quantum PC looks set to change a wide scope of businesses and applications. Many processing applications with enormous datasets are ready to profit by the appearance of the quantum PC and a lot of what the world does depends on the standards of science – from reproduction to application. The difficulty is, maths can be hard. A few counts required for the successful re-enactment of genuine situations are essentially past the ability of traditional PCs – what's known as immovable issues. Quantum PCs, with their tremendous computational force, are obviously fit to tackling these issues. To be sure, a few issues, as are considering, "hard" on an old-style PC, yet are "simple" on a quantum PC. This makes a universe of chances, across pretty much every part of present day life.(Spector, Barnum et al. 1999)

HealthCare:

Research:

Traditional PCs are restricted as far as the size and multifaceted nature of particles they can mimic and look at (a basic procedure in early medication improvement). In the event that we have a contribution of size N, N being the quantity of particles in the inquired about particles, the quantity of potential associations between these molecules is exponential (every iota can interface with all the others). Quantum PCs will permit a lot bigger particles to be reproduced. Simultaneously, scientists will have the option to show and re-enact connections among medications and every single 20,000+ protein encoded in the human genome, prompting more prominent headways in pharmacology.(Mohseni, Read et al. 2017)

Diagnosis:

Quantum innovations could be utilized to give quicker, progressively exact diagnostics with an assortment of uses. Boosting AI abilities will improve AI – something that is now being utilized to help design acknowledgment. High-goals MRI machines will give more noteworthy degrees of detail and furthermore help clinicians with screening for ailments.

Treatment:

Directed medicines, for example, radiotherapy, rely on the capacity to quickly demonstrate and mimic complex situations to convey the ideal treatment. Quantum PCs would empower advisors to run more reproductions in less time, assisting with limiting radiation harm to sound tissue.

Circuit, Software, and System Fault Simulation

At the point when one grows huge programming programs with a huge number of lines of code or enormous ASIC chips that have billions of transistors, it can get horrendously troublesome and costly to confirm them for rightness. There can be billions or trillions of various states and it is inconceivable for an old style PC to check each and every one in recreation. In addition to the fact that one wants to comprehend what will happen when the framework is working ordinarily, yet one likewise needs to comprehend what occurs if there is an equipment or other mistake. Will the framework recognize it and does it have a recuperation system to alleviate any conceivable issue? The expenses of a mistake can be high since a portion of these frameworks can be utilized where lives or a huge number of dollars may be reliant on their being sans blunder. By utilizing quantum processing to help in these recreations, one can conceivably give a vastly improved inclusion in their re-enactments with an enormously improved chance to do as such.

Cyber-Security

Digital security is turning into a bigger issue each day as dangers around the globe are expanding their capacities and we become increasingly powerless as we increment our reliance upon computerized frameworks, get familiar with cybersecurity in 2019 over at locales, for example, Upskilled and others. Different procedures to battle digital security dangers can be created utilizing a portion of the quantum AI approaches referenced above to perceive the dangers prior and moderate the harm that they may do.

Logistics and Scheduling

Numerous basic advancements utilized in industry can be characterized under coordination's and booking. Think about the carrier coordination's administrator who needs to make sense of how to arrange his planes for the best assistance at the most minimal expense. Or then again the industrial facility chief who has a regularly changing blend of machines, stock, creation requests, and individuals and requirements to limit cost, throughput times and expand yield. Or on the other hand the evaluating administrator at a car organization who needs to make sense of the ideal costs of the considerable number of handfuls vehicle alternatives to expand consumer loyalty and benefit. Albeit, old style registering is utilized intensely to carry out these responsibilities, some of them might be unreasonably convoluted for a traditional processing arrangement while a quantum approach might have the option to do it.

Financial Portfolio Optimization

Finding the ideal blend for a basketful of speculations dependent on anticipated returns, hazard appraisals, and different components is a day by day task inside the account business. Monte Carlo recreations are continually being sudden spike in demand for traditional PCs and devour a tremendous measure of PC time. By using quantum innovation to play out these computations, one could accomplish enhancements in both the nature of the arrangements just as an opportunity to create them. Since cash administrators handle billions of dollars, even a 1% improvement in the arrival is worth very much of cash. There is a site called Quantum for Quants that is committed to this subject you can look at to find out additional.

D-Wave Systems

D-Wave Systems offers its free Cloud Computing time to work on its quantum computers to help fight against COVID-19. Their work is towards finding of Vaccines, Therapies, and also to monitor its distribution as well as supply. D-wave Quantum computer uses an inbuilt Superconducting Circuits called as the SQUIDs (AKA Superconducting Quantum interface devices). Which shows tiny macroscopic quantum particles and also shows their properties as well.

D-Wave's 2000Q framework

D-Wave’s four frameworks discharged somewhere in the range of 2011 and 2017, territory in size from 128 to 2,048 quantum bits (qubits). A fifth framework, reported in September, will have 5,640 qubits and is, as per the organization's declaration, scheduled to be discharged in the not so distant future. Since 2018, D-Wave has offered remote access to quantum figuring through its "Jump" quantum distributed computing administration. It has a biological system of in excess of 1,000 designers has jumped up to apply Leap's quantum figuring assets to an assortment of purposes, including protein collapsing and money related demonstrating, and upgrading open transportation courses in Lisbon, Portugal. (Tanaka and Kashiwaya 1995)

D-Wave started offering an upgraded quantum figuring cloud administration (Leap 2) which couples recreated qubits (on an ordinary PC) with D-Wave's real qubits. The first Leap quantum cloud could just help issues containing all things considered 100 factors. What's more, those 100 factors must be scantily associated with each other. Jump 2, on the other hand, can bolster issues with up to 10,000 factors—which can all be completely associated with each other. (Borkowski and Hirschfeld 1994)

To delineate the contrast between "meagrely associated" factors and "completely associated" factors, For an example: An aircraft, state, has an armada of 100 planes spread out more than 25 air terminals, with 500 group individuals who are either flying the plane or overhauling the travellers or on the ground adjusting the planes. The ideal arrangement of timetables for those planes and staff individuals includes both the crude parameters above just as true requirements on the planes (upkeep calendars, climate, and number of compartments accessible at some random air terminal) and on the group (command posts, confirmation levels on different air artworks, work and excursion plans). Those requirements would be modified into a D-Wave calculation as degrees and sorts of connectedness between the factors.

Similarly, as with the Example above, the variables deciding every individual patient's transportation—regardless of whether it's because of the state of the patient or the quantity of staff accessible on some random move—can make the difficult complex.

The problems seen are explored in the following areas:

1) The modelling and simulation of the spread of the virus.

2) The scheduling of nurses and other hospital resources.

3) Assessing the rate of virus mutation.

4) The assessment of existing drugs as potential treatments.

How Can Quantum Computers Save us From COVID-19:

A group of analysts at Penn State University as of late started investigating powerful answers for sedate disclosure in order to stumble upon the remedy for COVID-19. Many other research groups, including those upheld by large tech and enormous pharma, are working a similar issue. In any case, this investigation is extraordinary. The Penn State group is carrying quantum AI to the battle.

Customarily, tranquilize disclosure's been a meticulous procedure including experimentation. We're talking eyeballs on magnifying instruments, pen and paper charts, and a huge number of distinct negatives for each conceivable positive. The appearance of profound learning speed things up a piece.

Superior registering, for example, supercomputers and man-made consciousness can help quicken this procedure by screening billions of concoction mixes rapidly to discover significant medication up-and-comers. This methodology works when enough synthetic mixes are accessible in the pipeline, however lamentably this isn't valid for COVID-19. This venture will investigate quantum AI to open new abilities in tranquilize disclosure by creating complex mixes rapidly.

Quantum Machine Learning to fight COVID-19:

Months into the COVID-19 pandemic, supercomputers crunching the coronavirus is the standard, not the special case. A large portion of these frameworks are centred around different components of a comparable way to deal with antibody or helpful revelation: screening mixes to perceive how unequivocally – if by any stretch of the imagination – they cling to the infection's spike protein or principle protease. Scientists are wanting to consolidate this burdensome procedure of medication improvement, which can regularly take numerous years or even decades, into under two years' time utilizing the animal power intensity of the world's most remarkable PCs.

With regards to finding an antibody that can end and kill the savage COVID-19 infection, the present supercomputers can unfortunately do a limited amount of a lot. While supercomputers can do astonishing things, they are not intricate enough to discover answers to nature's most profound and most entangled privileged insights, for example, rapidly and cautiously mapping out the sub-atomic structures of infections so they can be crushed with present day medications and medicines. Be that as it may, an answer anticipates maybe five to 10 years away as quantum PCs, which are exponentially more remarkable than conventional great PCs, as per PC researchers and different specialists.

As of late an open private association was shaped to make a COVID-19 High Performance Computing Consortium, which is attempting to saddle the intensity of superior registering assets to greatly speed up and limit of coronavirus explore. What's more, however that work is today welcome in the battle against COVID-19, it won't open all the unbelievably troublesome privileged insights that are held intently by such infections. For most pharmaceutical organizations, supercomputers are utilized routinely to help research, find, and recognize new medication medicines, including the distinguishing proof of infection structures so fixes can be found.

However supercomputers utilized today in infection and other pharmaceutical research are as yet dependent on old style processing designs that see all information as a progression of double bits with an estimation of zero or one. Those machines face the confinements of present day bit-based PC models and force that is accessible today yet can't hypothetically or truly handle all the enormously point by point inquire about that is as yet required.

Although the speculations made in theory that quantum computers can find solution to some of the hard problems that has been unsolved since last 50 years. In other words, proving whether P problem is equal to NP complete problem or not. Since all these years, we have been only able to prove a solution and with quantum computers we will be finally able to find a solution of a problem (Aaronson 2008). Some of the limitations that the quantum industry faces are as follows: (Ardabili, Mosavi et al. 2020)

No -cloning theorem:

This quantum computer law prohibits to make copy of information embedded in particles. If the information is accessed by an attacker or an intruder, distorted information will be received by receiver. It will take to break laws of quantum physics to access the information or the attacker has insider information. The fundamental property of physics on which the quantum teleportation works is entanglement between particles. According to the basic principle of quantum mechanics, only one result can be obtained out of all the entangled states. The remaining information gets irreversibly destroyed. This drawback is holding back quantum industry to build a commercial quantum computer having enough qubit to perform commercial used operations. (Bužek and Hillery 1996)

General Use of Quantum computers:

As in 1960 when first computer was invented, they used to perform very handful of tasks after number of operations equal to today's hand calculator. There were very few scientists who could operate the computer and it used to be tiresome to operate so many operations. Similarly, at present the real quantum computers also operate handful number of tasks which don't contribute to the common population. Services are available on cloud to hire a quantum computer for an hour or so to run complex tasks which will take ages to compute classically and one of the examples is IBM Q.

Complexity of Hardware:

The controlled environment in which all the phenomenon happens must be very cold refrigerator. The tubes and wire complexity are so high for the system is that a maximum of 54 qubit quantum computer has been built and experimented so far(Castelvecchi 2017). D-wave, an organisation in the competition of quantum computing has announced to build a quantum computer with 2000 qubit. If this announcement become reality, then half the quantum computer will outperform all the computers combined. New cryptographic methods will be needed to be deployed such as cryptanalysis and quantum cryptography to secure information. New data structure will be launched to sort, search and other problems to solve.

Common algorithms in machine learning and their quantum accelerations are as follows:

Algorithms	Quantum complexity
Bayesian Interference	O(√n)
Perceptron	O(√n)
Least square estimation	O(log(n))
Quantum principal component analysis	O(log(n))
Quantum SVM	O(log(n))
Quantum Reinforcement learning	O(√n)

(Petschnigg, Brandstötter et al. 2019)

Decoherence:

The Interaction of Qubits causes the changes in the behaviour, Decay and resulting in disappearing is called as the decoherence. Usually the quantum states are extremely fragile. If there is slightest change in the temperature or the vibration of the particles then disturbances are created which is known as Noise in Quantum terms. That's why quantum bits are to be protected from these external factors which effect the particles. Researchers take extreme care of the Quantum particles from outside world by using supercooled fridges and Vacuum chambers.

After all the efforts put in to reduce the noise, there is still some errors occur to creep into the calculations. To negotiate these errors a greater number of Q-bits are need to be used. However, it takes thousands of the standard bits to make a Q bit.

To exhibit superconductivity, the particles (electrons, protons, photons) needs to be in a controlled environment. The controlled environment is a vacuum space where the circuit is placed with absolute 0-degree temperature or -273 degree Celsius. The particles in the circuit should be free from radiation and noise. The Interaction of Qubits causes the changes in the behaviour, Decay and resulting in disappearing is called as the decoherence. Usually the quantum states are extremely fragile. If there is slightest change in the temperature or the vibration of the particles, then disturbances are created which is known as Noise in Quantum terms. That’s why quantum bits are to be protected from these external factors which effect the particles. Researchers take extreme care of the Quantum particles from outside world by using supercooled fridges and Vacuum chambers.

After all the efforts put in to reduce the noise, there is still some errors occur to creep into the calculations. To negotiate these errors more number of Q-bits are need to be used. However it takes thousands of the standard bits to make a Q bit. It’s a very expensive process in all aspects financially. This is the reason, very handful of companies are participating in to contribute. According to the paper published, a team in University of New South Wales (UNSW) Sydney has founded a way to conduct superconductivity in a fraction less than absolute zero-degree temperature quoted in a paper (Phys.org.). Today it might feel like nothing, but the technology gets the right supervision it can save millions of dollars in quantum computing devices. (Shor 1995)

Quantum Supremacy:

It's where a quantum Computers can finish a scientific computation that is certifiably past the scope of even the most remarkable supercomputer. It's as yet indistinct precisely what number of qubits will be expected to accomplish this since analysts continue finding new calculations to help the exhibition of old-style machines, and supercomputing equipment continues improving. In any case, analysts and organizations are endeavouring to guarantee the title, running tests against a portion of the world's most impressive supercomputers. There's a lot of discussion in the examination world about exactly how noteworthy accomplishing this achievement will be. As opposed to trust that incomparability will be announced, organizations are as of now beginning to explore different avenues regarding quantum PCs made by organizations like IBM, Rigetti, and D-Wave, a Canadian firm. Chinese firms like Alibaba are likewise offering access to quantum machines. A few organizations are purchasing quantum PCs, while others are utilizing ones made accessible.(Harrow and Montanaro 2017)

Temporal Modes:

Temporal modes are field-symmetrical ghastly worldly amplitudes of light heartbeats, for example Hermite-Gauss capacities. They structure a high-dimensional premise which can be utilized for organized quantum data applications.
There are a few angles that render transient modes engaging premise states. They can be thickly stuffed in time-recurrence space, they are normally good with single-mode filaments, and, because of their beat nature, they loan themselves to exact planning estimations. To completely

open their latent capacity, be that as it may, two requirements must be satisfied: first, we need the capacity to produce photonic quantum expresses that show a custom fitted transient mode structure; second, we need implies for controlling and estimating said structure. We can address the principal challenge by conveying scattering built parametric down-transformation (PDC). Utilizing our gathering speed coordinated PDC source as essential apparatus, we create photon-pair states with all around characterized dimensionality and client controlled Temporal mode appropriation. To do as such, one just needs to shape the complex range of the siphon beats, which implies that a difference in activity mode, state from single-mode to few-mode, doesn't require any extra test overhead.

The subsequent snag can be overwhelmed by utilizing an alleged quantum beat entryway (QPG, a gadget that is based on scattering-built entirety recurrence age. The QPG chooses a solitary transient mode from a multimode input signal, which is then changed over to an alternate recurrence; every other mode is transmitted. The specific state of the chosen mode is characterized by, once more, melding the perplexing range of the solid siphon beats.

Having these devices close by, we can show applications that utilization Temporal modes as premise states, where we recognize two general methodologies. When attempting to legitimately quantify the worldly waveform of a solitary photon, the QPG can be utilized to test this dissemination. It can likewise fill in as an interpretation gadget that joins recurrence moving from media transmission to noticeable frequencies and Temporal amplification of an info single photon. In this setup, the changed over photon is identified with a streak camera, a gadget that consolidates extraordinary worldly goals of a couple of picoseconds with single-photon affectability.

On the other hand, we can utilize the QPG to actualize a projective estimation onto subjective worldly mode superpositions, on the off chance that we are keen on the ghastly structure of the quantum light under scrutiny. This capacity permitted us to play out a worldly mode quantum state tomography of custom fitted proclaimed single photons from PDC. It can likewise be utilized to understand the dynamic control of the worldly mode structure of these photons. At long last, because of its characteristic stage affectability, the QPG can be utilized to perform high-accuracy time and recurrence estimations that outperform the goals of standard force estimations.

All in all, we have developed a tool kit that awards access to the worldly mode level of opportunity of quantum light. Custom fitted state age is accomplished in scattering built parametric down-transformation, though Temporal mode control and estimation are acknowledged with a quantum heartbeat door. These gadgets are empowering agents for novel .Quantum data applications, for example, transient mode quantum state tomography and high-accuracy time frequency estimations.(Brecht, Reddy et al. 2015)

Quantum devices to make contactless payment secure:

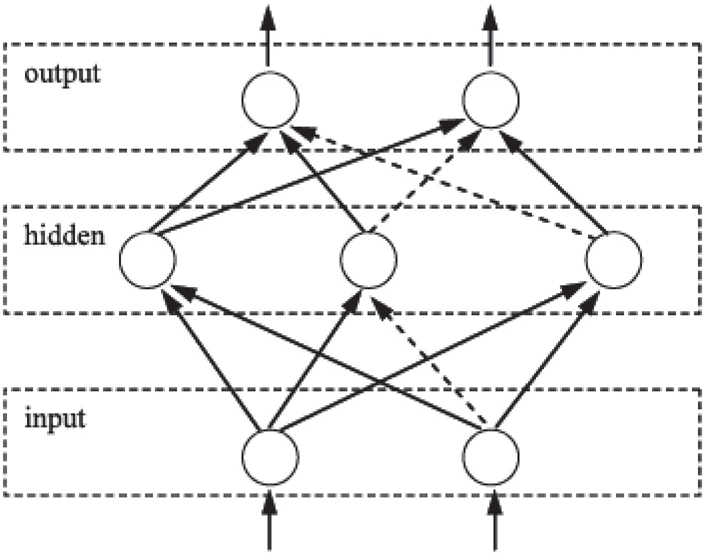
Usually when paying through mobile Phones, the mobile devices send a secrete key to the payment machines. So, these secrete keys must be encrypted to ensure it cannot be mis used. We can use quantum keys instead of secret keys to transfer the information from mobile phones to payment machines. Quantum technology uses millions of small particles present in light to transfer their encrypted keys. This procedure can detect even eavesdropping and can prevent hacking as well. If we use light to send the signals it is difficult for hackers to obtain information. The only way in protecting information is to ensure the data travels straight from sender to receiver. (Chun, Choi et al. 2017)

Quantum hacking: If use of quantum gadgets become a reality it opens a wide range of new attacks. Regular Side channel attacks might be less likely to happen, but new side channel attacks might occur. As of now the known quantum attacks are the Photon number splitting attacks and beam splitting attacks. There are also other channel attacks which are likely to appear. Quantum theory can explain how to deal with all those attacks theoretically but practically if the quantum gadgets become a reality then we have to deal with these attacks.(Wallden and Kashefi 2019)

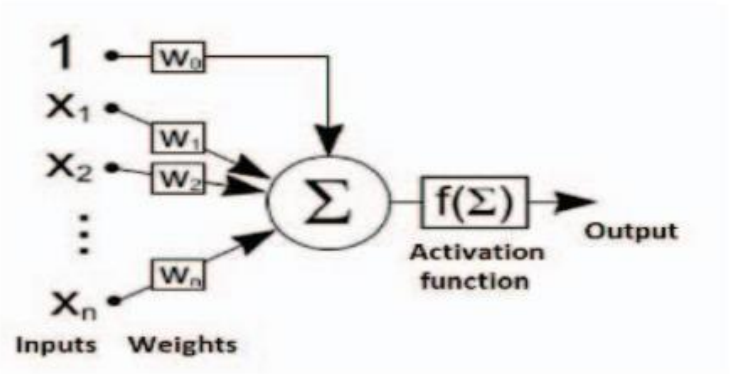
Alternative Approach:

Artificial Neural network:

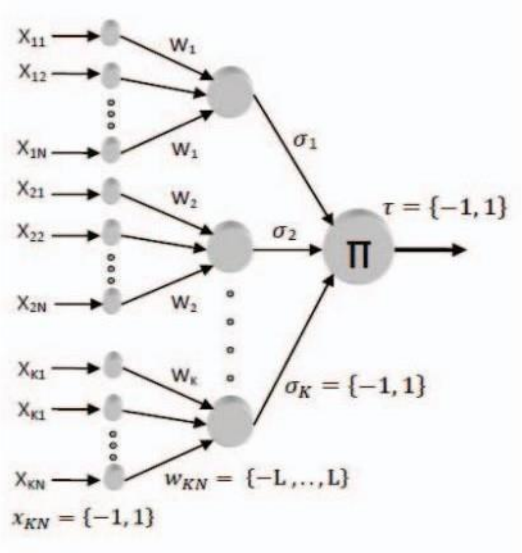
Artificial neural network is an information processing model taken from biology where neural network has an important task in human body. The key module of this structure is its information processing system. It is a collection of large number of highly organized processing elements operational in unity to solve particular problems.{Sharma, 2016 #7}



A basic computational part is known as neuron, node or unit. It takes input from some other units, or maybe from an external source. Each input has a randomly initialized weight connected with it, which can be customized for learning process, unit calculates some function f of the weighted sum of inputs {ÖzÇakmak, 2019 #9}.



Neural key exchange process depends on the synchronization of the two TPMs.



COMPARITIVE ANALYSIS

We discussed 2 different cryptography techniques and we are going to do a comparative analysis on the basis of different areas. The detail comparison is shown in the table.

Based on the table we can certainly say that neural network is more feasible in implementing and can provide better outcome as compare to quantum cryptography {Sharma, 2016 #8}.

	Neural Cryptography	Quantum Cryptography
Methodology	Combination of neural network concept from biology and cryptography	Combination of laws of quantum physics and cryptography
	ANN is used to depict the neural network	Heisenberg's uncertainty principle and the principle of photon polarization are the two fundamental laws on which whole technique is based
Used in	used for secret key exchange generated through tree parity machine by synchronization. And the encryption is done through various cryptographic encryption algorithms	used for the secret key generation through quantum cryptography protocols such as BB84 protocol, which is communicated over quantum channel, and finally the key is used for encryption with classical cryptography techniques
Advantage	The advantages of this system are that it is difficult to break without knowing the network architecture.	Random key generation
	Noise Tolerance	more secure cryptography than public key cryptography, can tackle big data effectively
	Message misrepresentation chances are very low	allows secure allocation of random key information among two partners
Disadvantage	Only effective where the key is the weight and the network architecture	High bit error rate
		point to point link
		lower key allocation rate
		serve up to limited distance

Methodology:

To study the writing of the field, a hunt is led with the accompanying models.

- Keywords utilized for looking through the significant writing incorporate "Cryptography" "Applications" and "Entanglement" as the exploration theme is about the Advantages of Quantum Computers over classical and also Advantages of Quantum Cryptography over classical Cryptography. Albeit some different catchphrases have been attempted, they have not spread the normal outcomes. Meanwhile, these three chose catchphrases have produced papers which are identified with the issue area directly.

- The primary sources which are utilized in the inquiry incorporate IEEE Xplore Digital Library and ACM Digital Library as they are the two most well-known computerized libraries in software engineering and figuring with driving exploration works. What's more, the full-writings of papers from these libraries can be accessed with the college understudy right. The chose catchphrases are utilized in the question string to recover the writing in these libraries. Every single relating distribution are thought of yet the consideration is put significantly more on "Early Access Articles" and the papers which have been distributed since 2014 with the goal that the chosen explores can mirror the present circumstance of the field. At that point, the outcomes are assessed, chosen, and broke down for the writing overview reason. For the chosen assets, to dissect widely, different quests are done to gather increasingly related papers to these papers. In addition, to give per user's essential instruments to settling open issues in the security field, protection saving procedures and their applications in the training are examined in detail. The EndNote electronic database is utilized to store and deal with the indexed lists.

Research and work:

With an influx of huge amount of data, we are not capable enough to cope with the problem of high processing need. Quantum computing offers many advantages over binary computing for such types of problems, for example searching or optimizing over large solution sets [1]. The availability of quantum computers has made a significant impact in evolution of computing. And in the race to reach quantum supremacy, Google published in a paper they achieved it with the help of 53 qubit sycamore processor quantum computer, generating a random number in 200 seconds compared to 10,000 years of supercomputer (not computed practically). Other rivals such as IBM, Microsoft, Rigetti Etc have different opinions over quantum supremacy. The quantum computer can solve problems that supercomputers cannot, but the quantum computers lags behind in "multipurpose tasks" use. Table 1 will give an overview of quantum computing and classical computing:(Chuang and Yamamoto 1995)

Classical Computer	**Quantum Computer**
It is a large scale integrated multi-purpose computer.	It is high speed parallel computer based on quantum mechanics
Information storage is bit based on based on voltage or charge.	Information storage in qubits based on electron spin.
Computers run on bits i.e. 0 or 1.	Computers run on qubits which
Two bits of computer act independently.	Qubits can be influenced by other qubits.
Same output will be gained in case of repeated computation on the same input. Deterministic i.e. 0 or 1.	Our confidence increases through repeated computation. Continuous I.e. output between 0 and 1.
Information processing is done by logic gates.eg: and, or, not.	Information processing is done by quantum gates on parallel basis.
Circuit behaviour is controlled by classical physics.	Circuit behaviour is governed by Quantum physics.

Operation are defined by Boolean algebra.	Operations are defined by linear algebra over Hilbert space.
No restrictions on cloning or measuring signals.	There are restrictions on cloning and measuring signals.

Table 1: Classical Computer vs Quantum Computer

Challenges faced by quantum computing:

Today Quantum computing is exactly at the same point as it was in the case of classical computer in 1960’s which is used to be of a room size. The only difference is that the growth is exponential in terms of research, progress and results. The major challenges for quantum computing include Quantum computer needs absolute zero temperature to conduct super conductivity. The use is not widely accepted due to its size and limitations to the type of jobs it can do. The questions that needs to be answered are How superconductivity can be performed at non-absolute temperature, and how it can perform the multipurpose task for which we use the classical computers.

The strength of quantum computing lies within the basic model on which it operates “Qubits”, it works on the principle of superposition which means the qubit can take either 0 or 1 at the same time. This property brings the increment in power for computation exponentially ($2^{?}$) where n is number of qubits. The current practical achievable value of n is 53 by google and it claims quantum supremacy. In response to Googles claim a company called D-Wave has announced a 5,000-qubit quantum computer to achieve quantum supremacy. Imagine the power of a computer which can solve a problem with a complexity of 2^{5000}.

In a recent study, a team in UNSW Sydney lead by Prof. Andrew Dzurak said “New results open a path for real world application of quantum computing in business and governance”. The researchers came up with the term “Hot Qubit” which operate at higher temperature compared to “Qubit” which works at a fraction below absolute 0. The researcher’s quantum processing unit cell works at 1.5 kelvin or 15 times warmer than the chip-based quantum computers such as Google’s and IBM’s. Although 1.5 kelvin is still very close but it can save millions of dollars in just refrigeration of qubits (Bernstein 2009).The technology has the potential to make a valuable contribution to the network security among government, businesses, and academic environment.

Quantum memories are the place where we can store Q-bits. The storage of the bits require larger storage units and also these units must be highly efficient and also higher bandwidth requirements. This is the reason it is harder to build a quantum memory. Solid state quantum memories with rare earth materials can be used in building of quantum memories (Arun and Mishra 2014).

Limitations:

There is no doubt that Quantum computers would be exponentially fast in processing and solving problems efficiently compared to classical computers but only with a few margins. The common mistakes that has been made related to quantum computers are claiming that It can solve difficult Mathematical anomalies in less time in comparison to classical computers. These claims are speculations and not achieved practically{Aggoune, 1989 #10}. According to our understanding Quantum computer will suffer from same hardships as classical computers in map problem (NP- Complete). Other than these theoretical problems, the two major problem that arise in practical Implementation of quantum computing are given below:

- Elements In the circuit needs zero decoherence I.e. the environment should be free from all kind of radiation and noise. This property prevents the computer from outside attack and loss of Information.
- Elements in the circuit needs absolute zero temperature to conduct superconductivity which is very expensive.

The fast processing power of quantum computers come from the fundamental structure of the computers i.e. qubits. Qubits are the particles which carry information in the form of spin. A Particle can be an electron with “spin up” representing 0, “spin down” representing 1 and superposition of both states simultaneously storing information. Small number of particles can carry huge amount of information, a mere 500 particles in a superposition represent each number from 1 to 2^{500} and the computer can execute those numbers parallelly to find solution for high complexity mathematical problems. The only drawback is that when we try to measure one of the final states of the particles the information of the particles gets lost and it is because of the property called “entanglement”. Entanglement is referred as the interaction between the particles i.e. state of one particle affects the state of other particles which helps in teleportation of information.

There has been claims since the first idea for quantum computers came up that the computers will be able to find the solution for hard NP- Complete problems. (Aaronson 2008)The scientists have divided the problems in different sections based on steps it will take to the final solution which are as follows:

1) P- problems: This section includes problems such as graph connectivity, finding whether the number is prime or not. These types of problems can be efficiently solved by quantum as well as classical computers. It’s easy to solve P problems on classical computers because the complexity increases relatively slow compared to other types of problems.
2) NP-problems: This section includes problem like factorization, graph isomorphism. There is no known algorithm of Classical computers can solve problems like factoring because complexity increases as the number “n” for factorization gets bigger. For such types of problems quantum computers are claimed to be efficient as it can handle the problem by solving it parallelly.
3) NP- complete problems: This section includes problems such as box packing, map colouring, travelling salesman problem. As of now there are no known algorithms which can solve such problems neither in classical computer nor in quantum computers.

The only solution available is black box approach i.e. hit and trail method.(Ohliger, Kieling et al. 2010)

4) BQP Problems: Although Quantum computers cannot solve all the problems on NP problem, quantum computer is able to solve some of the problems which classical computer cannot in ages. This type of category is known as Bounded Error Quantum – Polynomial time. It constitutes of all p problems and some np problems {Aaronson, 2008 #4}.

Theoretically, Quantum computers excel classical computing in processing and storing information which is directly proportional to number of qubits. Practically, it becomes difficult to construct a quantum computer with large number of qubits as it involves complex wiring and hardware. At present, the highest number of qubits in a quantum computer practically possible is 53 qubit sycamore processor.(Brooks (2019) Although with such promising future of quantum computers, they are going to excel our expectations but only marginally.

Conclusion:

The future of quantum computing looks bright as quantum computing has many applications like quantum cryptography, Teleportation of information. It also can be used in development of medicines by studying molecular behaviour, It also can be used in satellite communications as well. However, we hope that the theory becomes practical someday so we can use its advantages in many other fields of science.

The conclusion of the Thesis is that quantum computing is one of the huge opportunities for the modern world to open up the doors for unanswered questions. It promises to solve problems which classical computers practically cannot. But the cost behind quantum computing is too high. The major challenges that stands right now is to reduce the cost so that it is more accessible for experiments. And a significant progress has been made in UNSW Sydney which will save millions of dollars. Other challenges include to make a hybrid computer which can operate high processing jobs simultaneous with classical computing jobs which will open the opportunity to business and commercial use.

But in practice, getting enough qubits to work together to run any such algorithm — in what is known as a universal quantum computer — has proved extremely challenging. Two technologies have emerged as front-runners for handling qubits. One traps individual ions in a vacuum using electric and magnetic fields; the other incorporates qubits into microscopic superconducting circuits kept at a few degrees above absolute zero. IBM has bet heavily on the latter approach. Monroe has co-founded a start-up called IonQ that expects to roll out a cloud-based, trapped-ion quantum service, but he won't speculate on when. Google plans to do the same with its own superconducting-qubit machines, but only after it has made a working 50-qubit computer

References:

1. Aaronson, S. (2008). "The limits of quantum." Scientific American **298**(3): 62-69.

2. Ardabili, S. F., et al. (2020). "Covid-19 outbreak prediction with machine learning." Available at SSRN 3580188.

3. Arun, G. and V. Mishra (2014). A review on quantum computing and communication. 2014 2nd International Conference on Emerging Technology Trends in Electronics, Communication and Networking, IEEE.

4. Barends, R., et al. (2014). "Superconducting quantum circuits at the surface code threshold for fault tolerance." Nature **508**(7497): 500-503.

5. Barrett, J., et al. (2005). "No signaling and quantum key distribution." Physical review letters **95**(1): 010503.

6. Bennett, C. H., et al. (1992). "Experimental quantum cryptography." Journal of cryptology **5**(1): 3-28.

7. Bernstein, D. J. (2009). Introduction to post-quantum cryptography. Post-quantum cryptography, Springer**:** 1-14.

8. Borkowski, L. and P. Hirschfeld (1994). "Distinguishing d-wave superconductors from highly anisotropic s-wave superconductors." Physical Review B **49**(21): 15404.

9. Brecht, B., et al. (2015). "Photon temporal modes: a complete framework for quantum information science." Physical Review X **5**(4): 041017.

10. Brooks, M. (2019). "Beyond quantum supremacy: the hunt for useful quantum computers." Nature **574**(7776): 19-21.

11. Bužek, V. and M. Hillery (1996). "Quantum copying: Beyond the no-cloning theorem." Physical Review A **54**(3): 1844.

12. Chuang, I. L. and Y. Yamamoto (1995). "Simple quantum computer." Physical Review A **52**(5): 3489.

13. Chun, H., et al. (2017). "Handheld free space quantum key distribution with dynamic motion compensation." optics express **25**(6): 6784-6795.

14. Cross, A. (2018). "The IBM Q experience and QISKit open-source quantum computing software." Bulletin of the American Physical Society **63**.

15. Feynman, R. P. (1986). "Quantum mechanical computers." Found. Phys. **16**(6): 507- 532.

16. Gisin, N., et al. (2002). "Quantum cryptography." Reviews of modern physics **74**(1): 145.

17. Gottesman, D., et al. (2004). Security of quantum key distribution with imperfect devices. International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings., IEEE.

18. Goyal, A., et al. (2011). Quantum Cryptography & its Comparison with Classical Cryptography: A Review Paper. 5th IEEE International Conference on Advanced Computing & Communication Technologies [ICACCT-2011].

19. Grosshans, F., et al. (2003). "Quantum key distribution using gaussian-modulated coherent states." Nature **421**(6920): 238-241.

20. Gruska, J. (1999). Quantum computing, Citeseer.

21. Gu, X., et al. (2017). "Microwave photonics with superconducting quantum circuits." Physics reports **718**: 1-102.

22. GUANCO, F. (2015). "What is Quantum Key Distribution." Cloud Security Alliance.

23. Häffner, H., et al. (2008). "Quantum computing with trapped ions." Physics reports **469**(4): 155-203.

24. Harrow, A. W. and A. Montanaro (2017). "Quantum computational supremacy." Nature **549**(7671): 203-209.

25. Hines, J. (2018). "Stepping up to summit." Computing in science & engineering **20**(2): 78-82.

26. Inamori, H., et al. (2007). "Unconditional security of practical quantum key distribution." The European Physical Journal D **41**(3): 599.

27. Jennewein, T., et al. (2000). "Quantum cryptography with entangled photons." Physical review letters **84**(20): 4729.

28. Kamra, S. and J. Scott (2019). "Impact of Data Breaches to Organizations and Individuals." Available at SSRN 3510590.

29. Leuenberger, M. N. and D. Loss (2001). "Quantum computing in molecular magnets." Nature **410**(6830): 789-793.

30. Lo, H.-K. and H. F. Chau (1997). "Is quantum bit commitment really possible?" Physical review letters **78**(17): 3410.

31. Lo, H.-K., et al. (2005). "Decoy state quantum key distribution." Physical review letters **94**(23): 230504.

32. Ma, X. (2008). "Quantum cryptography: theory and practice." arXiv preprint arXiv:0808.1385.

33. Mohseni, M., et al. (2017). "Commercialize quantum technologies in five years." Nature **543**(7644): 171-174.

34. O'brien, J. L. (2007). "Optical quantum computing." Science **318**(5856): 1567-1570.

35. Ohliger, M., et al. (2010). "Limitations of quantum computing with Gaussian cluster states." Physical Review A **82**(4): 042336.

36. Politi, A., et al. (2008). "Silica-on-silicon waveguide quantum circuits." Science **320**(5876): 646-649.

37. Renner, R. (2008). "Security of quantum key distribution." International Journal of Quantum Information **6**(01): 1-127.

38. Scarani, V., et al. (2009). "The security of practical quantum key distribution." Reviews of modern physics **81**(3): 1301.

39. Shor, P. W. (1995). "Scheme for reducing decoherence in quantum computer memory." Physical Review A **52**(4): R2493.

40. Shor, P. W. and J. Preskill (2000). "Simple proof of security of the BB84 quantum key distribution protocol." Physical review letters **85**(2): 441.

41. Singh, J. and M. Singh (2016). Evolution in quantum computing. 2016 International Conference System Modeling & Advancement in Research Trends (SMART), IEEE.

42. Spector, L., et al. (1999). "Quantum computing applications of genetic programming." Advances in genetic programming **3**: 135-160.

43. Spiller, T. P. (1996). "Quantum information processing: cryptography, computation, and teleportation." Proceedings of the IEEE **84**(12): 1719-1746.

44. Steane, A. (1998). "Quantum computing." Reports on Progress in Physics **61**(2): 117.

45. Tanaka, Y. and S. Kashiwaya (1995). "Theory of tunneling spectroscopy of d-wave superconductors." Physical review letters **74**(17): 3451.

46. Van Assche, G. (2006). Quantum cryptography and secret-key distillation, Cambridge University Press.

47. Wallden, P. and E. Kashefi (2019). "Cyber security in the quantum era." Communications of the ACM **62**(4): 120-120.

48. Wasankar, M. P. P. and P. Soni (2013). "An invention of quantum cryptography over the classical cryptography for enhancing security." International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol **2**.

49. Woerner, S. and D. J. Egger (2019). "Quantum risk analysis." npj Quantum Information **5**(1): 1-8.

50. Xiang, Z.-L., et al. (2013). "Hybrid quantum circuits: Superconducting circuits interacting with other quantum systems." Reviews of modern physics **85**(2): 623.

51. Zhou, T., et al. (2018). "Quantum cryptography for the future internet and the security analysis." Security and Communication Networks **2018**.

View publication stats