IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10570

A Detailed Study on Cryptographic Systems in the Quantum Internet for Working Quantum Computers

Samiksha Shukla[1], Nimisha Sinha[2], Chetan Verma[3], Muddana Venkatesh Prasad Rao[4]

Professor in Department of Information Technology, Govt. Engineering College, Bilaspur, C.G. India[1]

Student in Department of Information Technology, Govt. Engineering College, Bilaspur, C.G. India[2-4]

Abstract: Quantum theory is one of the most fortunate theories that have influenced the course of scientific progress all through the 20th century. Quantum mechanics has given us the concept of quantum computers by using principles like superposition and quantum entanglement which seek to significantly boost the computational power and now it has become an evolution in classical computer science. We know that Current cryptography systems are based on the process called prime factoring which is vulnerable due to both significant enhancement in computational power and advancement in mathematics to reverse one way function like Shor's algorithm. To solve this problem, we need to induce quantum physics in current cryptographic system which leads us to the topic "Quantum Cryptography" which works on the principle of "Quantum Key Distribution". QKD is the scheme which allow the generation of shared private key, which can be used with a traditional encryption algorithm or as a one-time pad which encrypts each message for one time use key. But QKD only works if we can successfully transfer entangled quantum states or qubits over long distances perfectly intact, leading us to the concept of "Quantum Information Theory" or quantum internet. The scope of this paper covers concept of quantum computing, weaknesses of current cryptosystems, post quantum cryptographic system, fundamental concept of quantum cryptographic system and quantum information theory with challenges of implementing it in real world and its limitation and finally about upcoming future of transition of digital age to quantum age.

Keywords: Quantum Computers, Quantum Key Distribution, Quantum Information Theory, BB84 Protocol

I. INTRODUCTION

"Those who are not shocked when they first come across quantum theory cannot possibly have understood it" is a famous quote given by Niel Bohr. This quote demonstrates how revolutionary this theory is which has the capability to change the world. There are some rules in quantum physics which cannot be completely understood by regular physics like

1. The uncertainty principle which states that "There is a fundamental limit what one can know about the quantum system. For example, the more precisely one knows particle's position, the less one can know about its momentum, and vice versa."
2. The no-cloning theorem states that "It is impossible to create an independent and identical copy of an arbitrary unknown quantum state".
3. Quantum entanglement in which the quantum state of two or more objects has to be described with reference to each other, even though the individual objects may be spatially separated.

Around the world today, quantum theory has given us the concept of quantum computers which has the capability to transmogrify the whole field of computer science and ultimately human society.

II. NEED OF QUANTUM COMPUTERS

Since 1960's our computing power has grown tremendously resulting computers to get smaller and more powerful at the same time but this process is about to meet its physical limits as computer parts are approaching to the size of an atom now this is an problem as computer parts are made up of logic gates which is made up of transistor which works as a switch which can either allow electron to pass through it or completely block it , which is stored in the form of bits that is 0 or 1 .Combination of many bits are used to represent more complex information. Today a typical scale of transistors is 14 nanometres which is about 5 times less than a covid virus which is approximately 80 nanometres and about 500 times more than a red blood cell which is about 7000 nanometres. As transistors are getting smaller and smaller which is

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10570

only to the size of few atoms, electrons may transfer themselves to the other side of transistors even when the gates are close or we can say when the passage was blocked by a process known as “quantum tunnelling”.

A. *Quantum Tunnelling*

It is a quantum mechanical phenomenon when a particle is able to penetrate through a potential energy barrier that is higher in energy than the particles kinetic energy.

Now we are planning to use this physical barrier for our technological progress by introducing the concept of quantum computers. In normal computers we use bits to store any information but quantum computers use qubits or quantum bits to store any information. A qubit can be represented with different physics systems like the spin of an electron or the polarization of a single photon, 0 and 1 are their possible states like photon horizontal or vertical polarization. In the quantum world qubits don't need to be in any one state; it can stay in both the state of 0 and 1 by superposition theorem, but as soon as its value is tested it collapses into one of the definite states. Thus, n qubits manage information corresponding to all the possible 2^n permutations. This is the key to the massive computational power of quantum computers. For example, if we are given four bits of space, we can choose one from sixteen combination of ones and zeros, but with qubits which is a superposition of probabilities for 0 and 1, 4 qubits will be in all 16 possible combinations at once means we can use all 16 possible combinations together. A normal logic gate gets a simple set of inputs and produces one definite output but a quantum gate manipulates an input of superposition, rotates probabilities and produces another superposition as an output. This means we can get lots of calculation done parallelly which would be more efficient than would ever be possible on normal computer.

Quantum computers can be used in variety of fields like database searching, when normal computers can take days to search a file by using try and error method for each file whereas quantum computers algorithms will only take square root of that time. Another useful field is simulation, quantum simulations can provide new insights on proteins that can revolutionize medicine. Quantum computers can be used to revolutionize any field of science including space research programs, chemistry, AI and machine learning, math problems like prime factoring (which can lead to being a threat over current cryptography systems) and other extra fields.

III. Limitations of Current Cryptographic Systems

The logic gates of quantum computers exist in the state of superposition of many simulated configurations. This allows the computation of a certain type of calculation to be done in parallel and enormously faster than a normal computer. An example of this is how a quantum computer can compute the prime factor of a large number really fast. Now, this can be a problem as prime factorization is a key to modern cryptographic systems.

A. *RSA Protocol*

RSA (Rivest Shamir Adleman) is an algorithm used by modern computers to encrypt and decrypt a particular message in modern cryptography. It is an asymmetric cryptographic algorithm. This means it utilizes a pair of keys, a private key and a public key. The public key can be used for encryption and the private key for decryption. These keys are connected to one another via a one-way function. It's a mathematical function which is easy to calculate in one way (to find public key from private key) but really hard to calculate in the opposite direction (to gather the private key from the public key). Anyone can encrypt a message using a public key but it can only be decrypted by the recipient holding the private key.

In RSA protocol we choose two prime numbers, one of which is large, multiply them together (as their product is easy to compute) to get an even larger number and broadcast that as our public key and the recipient holding private key which is a prime factor of public key (as factoring of product is hard) can decrypt the message. All these functions work normally as long as it is harder to factorize the public key back to its prime, now for normal computers it will take years to compute that but with the introduction of quantum computers this can be done instantaneously. So, quantum computers can factorize public key quickly which leads to failure of modern cryptographic system.

B. *Shor’s Algorithm*

In 1994 a mathematician named Peter Shor developed an algorithm called Shor’s algorithm that could be used by a quantum computer to factor a prime number in an incredibly short amount of time. It turns out there is a structure of factorization that can be exploited by quantum computers that structure is period.

For example, let's consider power of 2 which is 2, 4, 8, 32, 64, 128, 256, 1024 … if we divide these powers by let say a random number 5 and look at remainder or mod, we will get 2, 4, 3, 1, 2, 4, 3, 1, 2, 4, 3, 1.

It repeats every four numbers. So, if we can figure out the period of this sequence, we can figure out the original number in this case which is 2. The 18th century mathematician Leonhard Euler figured this structure extends to numbers that

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10570

are multiple of 2 prime numbers- like the RSA algorithm. But for the power of large numbers guessing the period is as hard as guessing the number, this is where quantum computers come in and make it possible.

We know that normal computers are made up of bits that are 0 and 1, which is replaced by qubits in quantum computers. Now each qubit state represents a different state with different probability. It is like a parallel processor which is processing in different parts of quantum wavefunction. The problem with this parallel processing is that you only get one answer when you try to read out the qubits. If quantum computers are used to find prime factors one could read out guesses as a result. There is a way to boost the chance of getting the right answer by holding these repeating modules of Shor's algorithm- one per quantum state in the superposition in an array of qubits. Now, the entire superposition (all elements of wave-function) is related by the period of their repetition, which makes it possible to suppress the all-possible periods besides the correct one so we can say that ones we find the period we find the prime factors which ultimately results in failure of RSA algorithm.

Now the possibility of development of a quantum computer of practically useful size cannot be neglected. Then not only public key cryptography become insecure but it becomes insecure posteriorly: all encrypted messages from the past can be read. This creates an unacceptable risk for those applications of cryptography where data keeps value for a long time. It is important to notice that this technical advancement can happen behind closed doors of a government lab and may not be publicly announced at that very moment. In such a case, when it is announced that quantum computers have been built and public key cryptography is broken, it may be possible that all encrypted messages may not be safe.

Thus, the modern cryptographic system is convenient but risky. So, we are required to find one-way-function that don't have a known exploitable quality like the recurrence of prime factoring.

IV. POST QUANTUM CRYPTOGRAPHIC SYSTEM

Post quantum cryptographic systems refers to cryptographic algorithms that are secure against a cryptanalytic attack by a quantum computer or we can say these are the algorithms that are not based on the prime factorization due to its vulnerability towards quantum computers and Shor's algorithm.
In order to discover these kinds of algorithms there are many competitions currently running. One of them is by NIST, the National institute of Standards and Technology. One of the NIST finalists described an algorithm called McEliece cryptosystem.

A. *McEliece Cryptosystem*

McEliece cryptosystem is named after a cryptographer known as Robert McEliece. He discovered a math problem in 1970 and discovered this algorithm in 1978. This algorithm is based on the principle that it is really challenging to repair errors in large messages which give us a potential way to generate one-way-function.
In this cryptosystem the key is to modify the message in a reversible way so that we can create a large code word then add error to that code word. As it is hard to decode the encrypted message and even harder to decode it with the error induced in it. McEliece does this by coding messages into large matrices and scramble it using a key matrices and code your message into the result then adds errors to it, making it nearly impossible to decode the errors from the gigantic matrix. And because of the error it is impossible to brute force the one-way function in the backward direction. This way McEliece avoids the periodicity that makes RSA vulnerable to Shor's algorithm. Now we are currently not using this algorithm as the current cryptosystem because this uses a gigantic matrix as a public key which is around 8 mb which is 8,000 times larger than the current public key according to the RSA algorithm which is in order of some kb. So, this means that our current network protocols are not built to handle this. This can result in dramatic slowdowns in transactions.

B. *Lattice Based Cryptosystem*

Lattice based cryptosystems rely on the difficulty of problems like the shortest vector problem. Now, suppose we have an enormous field dotted regularly with points this is called lattice. If we are trying to cover the whole space by forming a giant parallelepiped. In order to find the shortest vector, or distance from one point to another point so far there was no classical or quantum algorithm to solve it quickly for large lattices. Now because of the large lattices, lattice candidates also have large public keys like McEliece cryptosystem.
This cryptosystem includes three of the other public key encryption finalists like NTRU, CRYSTALS-KYBER, and SABER.

Mathematicians and cryptographers are trying really hard to prove their encrypting and decrypting abilities. Post cryptographic algorithms seem hard for a quantum computer to crack but it does not mean no one will come up with a way to do it. So, besides all these, quantum cryptography is more promising and pretty darn secure if we had a quantum

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10570

internet. In the meantime, post quantum cryptography may be the only way to protect us from black hat quantum hackers.

V. QUANTUM CRYPTOGRAPHY

Rather than depending on the complexity of factoring large numbers, quantum cryptography is based on the fundamental principles of quantum mechanics which in fact rest on two pillars of quantum physics - the quantum entanglement and the Heisenberg principle. This principle plays a critical role in blocking the attempts of eavesdroppers in quantum cryptography. Charles H. Bennet and Gilles Brassard developed the concept of quantum cryptography in 1984 as a part of a study between physics and information. Quantum cryptography makes it possible for two parties to share a random key in a secure way.
The representation of bits through polarized photons is a foundation of quantum cryptography which serves the underlying principle of" quantum key distribution".

Quantum key distribution uses quantum properties to exchange secret information like a cryptographic key which can be used to encrypt message that are being communicate over the insecure channel. QKD addresses the challenges confronting classic key distribution approaches by proving a provably secure cryptographic building block to share cryptographic keys.

C. *BB84 Protocol*

While QKD does not solve the authentication problem, it does make undetected eavesdropping impossible. The uncertainty principle tells us that we cannot simultaneously know the value of certain pairs of properties, in this case a particle's position and momentum. These are called complementary or conjugate variables, an example of that is polarization of photons in quantum of electromagnetic waves. Polarization defines the direction of its electric and magnetic wave which can be either measured vertical versus horizontal polarization or diagonal versus other diagonal polarization. Now, rectilinear and diagonal polarization are complementary properties which means if we measure one we will lost all information about the other and a unmeasured photon exists in the state of superposition we can measure the state of photon by sending them to the polarization filter that can forces the photo to choose first between rectilinear or diagonal then in which direction. So, for example if we pass a randomly polarized photon though horizontal polarization filter, if it is horizontally polarized it will pass through it. If we put vertically polarized filter in front of that we will see nothing passes through but if we keep put third filter in between in 45 degree some photons pass through.
So here, we switched between different quantum representations of reality and then back again which invoked the uncertainty principle. So, after passing through the first filter the photon was rectilinearly polarized and when it reaches that diagonal filter it has a 50% chance of passing through it. As diagonal polarization is defined so again it has a 50% chance to traverse that third filter.

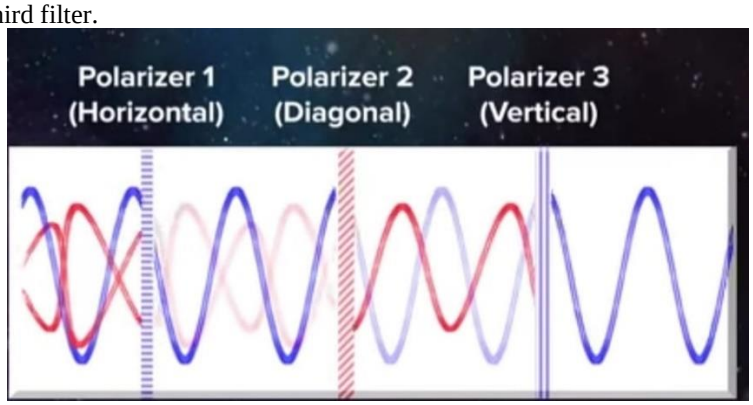

Fig 1 Pass of Randomly-Polarized Photon through Polarization Filters

This is the basics of the QKD algorithm developed in 1984 known as BB84 algorithm. This algorithm was proposed by Charles H. Bennett and Gilles Brassard, therefore got its name "BB84". This algorithm uses pulses of polarised light (each pulse contains a single photo). Suppose Alice and Bob are connected by a quantum channel more often an optical fibre and a classical public channel, now in order to provide a secure communication Alice who wants to send a message to Bob must choose between four possible non-orthogonal states.

- Horizontal vertical basis $\oplus$

1. Horizontally Polarized $|\leftrightarrow\rangle$
2. Vertically Polarized $|\updownarrow\rangle$

- Diagonal Basis $\otimes$

1. + 45° polarized $|\searrow\rangle$

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10570

2. – 45° polarized | ⤢⟩

Now imagine that Alice and Bob want to decide a private key for their messages. Now Alice generates a random string of bits 0's and 1's and encodes these bits using photons polarized in a particular way and uses a randomly chosen basis either rectilinear or diagonal for each of the photons. These bits are then sent over an open channel to Bob which is also known as "raw key" who then randomly picks a basis of his own for each photon and project onto that.
If he uses the same basis Alice did he gets the same result that would the one Alice send like first bit is one bob also gets first bit 1 otherwise he gets a random result.
Now over the same pubic channel they randomly pick a subset of those bits and Alice reveals which basis was used for those photons and what he sent. If bob used a different basis he ignores the result as he knows it will be random but if he uses same basis he should get same result.
For example, the following figure illustrates the process of the BB48 protocol. Where | ↕⟩ and | ⤢⟩ code for 1, while |↔⟩ and | ⤡⟩ code for 0.

Alice's polar. states	| ⤡⟩	| ↕⟩	| ↕⟩	| ↔⟩	| ⤢⟩	| ⤢⟩	| ↕⟩	| ⤡⟩	| ↔⟩
Alice's bit value	0	1	1	0	1	1	1	0	0
Bob's basis	⊗	⊗	⊕	⊗	⊕	⊗	⊗	⊕	⊕
Bob's measured states	| ⤡⟩	| ⤡⟩	| ↕⟩	| ⤡⟩	| ↔⟩	| ⤢⟩ /	| ↕⟩	| ↔⟩	
Bob's bit value	0	0	1	0	0	1 /	1	0	
Same basis?	Y	N	Y	N	N	Y /	N	Y	

Fig. 2 BB84 example

If someone let's say Eve, intercepted these messages, which were send on public channel did his own measurements, that would result in disturbance of system in such a way that Alice and Bob can find out. This is because like Bob, Eve can only pick a random basis each time on which to project the protons if he picks the right one. The photon state is unchanged and if he picks the wrong one it will project the photon into random state meaning bob isn't sure of getting same result even after using the same basis. In this way Alice and Bob can detect a man in the middle attack. Once they have done this test and verified that the information was not intercepted, they discard the no matching measurements and keep the rest each translated to bit depending on basis choice.
That gives a number which become their private key which is known only by them. It's possible for Eve to guess the exact basis as Alice and not disturb the state but chance is 1 in 2 to the power of the number of photons, which is close to impossible given that Eve only gets one shot. This makes eavesdropping on the channel impossible. These attacks are in principle as Eve could impersonate Alice and Bob from very start but there are authentication methods which makes this process really hard.

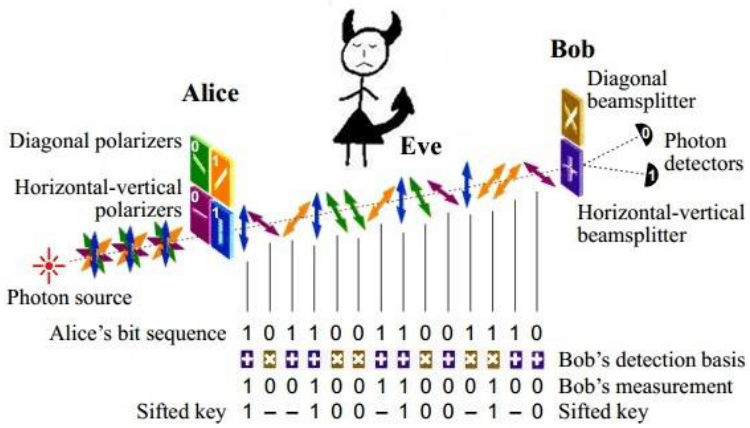

Fig. 3 BB84 Protocol Eavesdropping

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10570

D. Ekert Protocol

The Ekert Protocol was developed by Artur K. Ekert in 1991. This protocol uses simple quantum basic mechanisms but with added frills of quantum entanglement.it is also based on Bell's inequality. If we create a pair of particles with quantum properties which are correlated, for example electrons with opposite spin axes or photons with 90^{o} polarization, now our choice of direction will give directions to those particles.

In quantum entanglement we choose an basics to measure one of those particle let's say up down for spin and diagonal for polarization and the entangled particle also become measured, it will have exact opposite properties of that measured particle when measured in a same basis. Even though if that particle is measured in the different basis the result of the measurement will be correlated in such a way that it depends on the choose of measurement basis at both the end.

This phenomenon gives another way to transmit a secure key that way is Ekert protocol. The Ekert protocol, often also Einstein-Podolsky-Rosen protocol works as follows:

Now this time Alice creates a set of entangled particle pairs and transmits one half of those to bob. He then choses set of basis to measure its own particles now the choice of basis represents the set of bits. Bob then chooses a random set of basis to measure the particle he received. Now as these particles are entangled the outcome of Alice and Bob measurements should be correlated in a particular way defined by bells algorithm. In some cases, if that doesn't happen, they will know that the message was interrupted by someone, say eve because of the interruption, particles must be disentangled on route. In this way Alice and Bob can share the private key which is kind of similar to BB84 protocol.

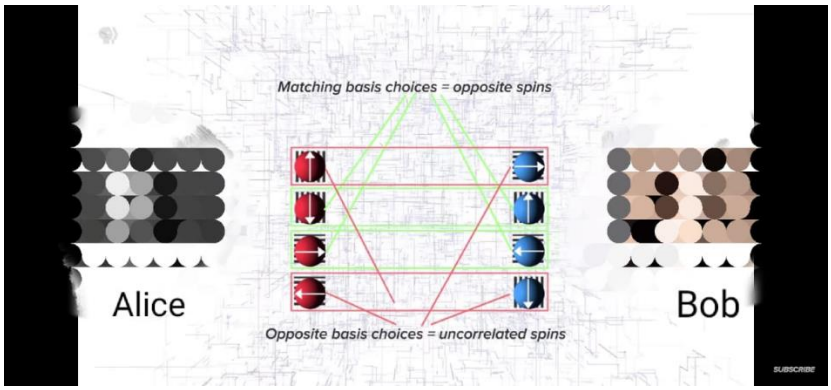

Fig. 4 Ekert Protocol Working Model

In the presence of quantum computers even the smartest classical protocol will be compromised. So we need QKD to work. In order for them to work we need to build a system where one quantum state and particularly entangled states can be transmitted. Or in simpler words in order for QKD algorithms to really work we need to build a quantum internet where we can transfer qubits which are notoriously fragile and really hard to transmit across large distances.

VI. QUANTUM INTERNET

Quantum internet or it can also be called as quantum information theory is similar to classical information theory but instead of using bits, it deals with qubits. In classical information theory we create, store and transmit information in the form of bits. In 1948 Clude Shannon published a paper called "A Mathematical Theory of Communication" which increased the rate of digital information which can be transferred without errors. In the quantum information system qubits have some fundamental prohibition on top of all the challenges of transmitting and storing quantum information. As we have already discussed QKD only works if we transmitted entangled qubits over long distances perfectly intact but here the problem is that to transmit quantum information we are required to pay attention to individual photons-quanta of light.

In order to transfer classical information using light, each bit is encoded with many photons from which many may be lost or altered on route without compromising the signal.

In such cases if too many photos are lost, we can just run the channel through a repeater which reads the signal and boost it with extra photons. Now, it is really difficult to transfer a single photo in such way with exactly maintains their quantum state and it is fundamentally not possible to make duplicates of those photons in order to boost the signal this is because of "No-Cloning Theorem" which states that it is impossible to take a quantum state and copy it perfectly and end up with two copies of same state existing at the same time. This Is in reference with the "Law of Conservation of Quantum Information" it states that every quantum state in the universe should be perfectly traceable that is from a single quantum state to a single quantum state both forward and backward in time which restrict a quantum state from vanishing but also splitting in two or being copied.

Now in reference to the no-cloning theorem, if we try to measure a qubit which we eventually have to do in order to make a copy of it, we disturb the quantum state in such a way that we never end up with two exact copies of a qubit, even if

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10570

are able to copy a qubit it would be nearly impossible to transmit it because the act of reading the state and copying it would destroy the entanglement through a phenomenon called “decoherence”. Now while it's nearly impossible to copy a qubit it is possible to overwrite it or we can say teleport it. Qubits can be overwritten with exactly the same state but in a completely different location which allows us to massively extend the range over which we can send an intact qubit where no copying and boosting is needed.

To understand that let’s consider a pair of entangled particles A and B created by robin and ted which can be received using a quantum channel. Now consider that Robin wants to send a qubit to Ted in order to do that robin performs a special type of measurement on that qubit called bell’s measurement. Let's say that qubit A and B are polarization states of two photons which are entangled, say one is vertically polarized and another is horizontally polarized. If we measure any one of them, we get the information of both of them.

Now robin takes photon A and entangles that with photon C using Bell's measurement which makes A and C to have opposite polarization. Photon B which was previously entangled with photon A will now have the same polarization as original photon C.so now we can say that the original quantum state of photon C which contains the message has been almost completely teleported to photon B. But our work here is not complete as there is more to the quantum state of C other than polarization which is fixed by entanglement. The remaining information of entanglement is obtained by study of the process that generated entanglement itself. Now this measurement outcome is encoded in 2 classical bits which robin sends to ted through classical channels. Using the information provided to Ted he then calculates its own measurements and reads the qubit C.

Here the minor problem is that it is not easy to perform Bell's measurement and extract all the information we need for this process using photonic qubits, but it can be done using matter qubits combined with a Quantum Key Distribution protocol. This process can be used to transmit quantum information over large distances. We will also be required to put some repeaters in the quantum channel.

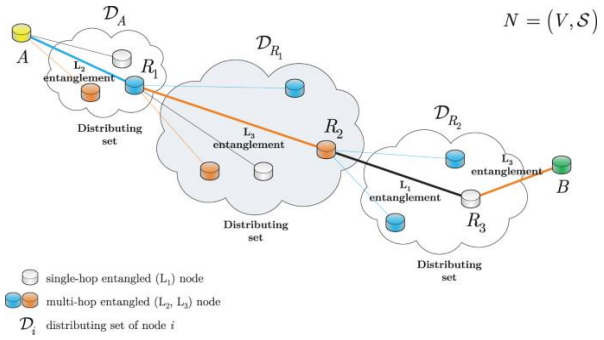

Fig. 5 Quantum Internet

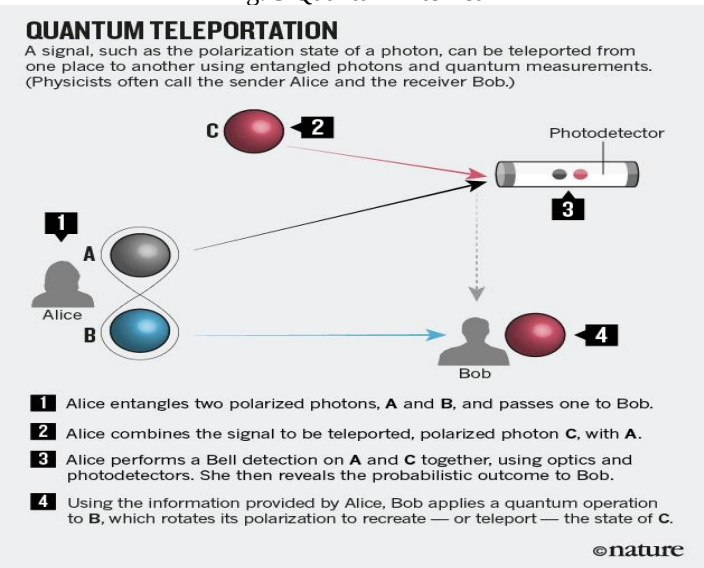

Fig. 6 Quantum Teleportation

A. *Implementation Challenges*

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10570

Quantum internet sounds fascinating but there are many challenges in its actual implementation like it is pretty much impossible to do all the transmission , entanglement study and measurements in perfect synchrony .
Now in the previous example we were storing quantum state and transferring it between photons and a matter particle, let's say an electron whose ups and downs spin direction can be entangled with the polarization state of a photon but it is really hard to store such delicate quantum information for any amount of time.
Experimentalists have some solutions for this problem ranging from storing the spin- state of a single electron in a nitrogen atom embedded in a diamond crystal or the entangled photon quantum state in a cloud of caesium atoms.
In upcoming years if we can maintain entangled states for long period then it may be possible for a group to establish a secure communication over a large array of multivalued entangled qubits which they can use to communicate with each other using bell's measurement it could be done in centralised node quantum switch board. There is also research going which eliminates physical storing devices with repeaters that are completely photonic which are enormously faster than our current stroking devices. Some scientists has also succeeded in bouncing entangled photos off a satellite ,there photons can then transfer there entangled states to other matter storage system which eventually do the job of repeater which extends the range and become a bridge to connect these quantum channels.

B. *Why is quantum information never lost?*
Newton's equation for classical mechanics ,Maxwell's equation for electromagnetism and Schrodinger's equation for quantum mechanics these laws can be used to predict how the universe will evolve into the future or we can say perfectly predicts how the system will change in the next instant and instance after that. But determinism in forward direction does not mean that the same law can be used to predict the past. We can say a system is in time -reversal symmetry if information about the configuration at all prior times exists, and always will even if we cant practically access it. That's the law of conservation of information.
The probability of a particle to be in somewhere should be sum to 1. That's the law of conservation of probability. And the unitarity states that the quantum states must remain independent of each other in order to preserve probability.so thats means two independent quantum state cant evolve into exact same quantum state if they did,then the probability for the initial state or for final state cant both sum to 1.so the only type of evaluation that preserves probability and unitarity is the evolution that also preserves the number of quantum states and preservation of quantum state means preservation of quantum information as we can trace quantum state in definectly forward and backward direction.

VII. IMPLEMENTING QUANTUM CRYPTOGRAPHY

There are some systems that have successfully implemented quantum cryptographic technology which are:
A. *The DARPA Quantum Network*
The DARPA Quantum Network demonstrates that quantum cryptography may indeed be used, in practice, to provide continuous key distribution for Internet virtual private networks. DARPA is a cryptographic Virtual Private Network (VPN). It is a security model that augments or completely replaces the existing VPN key agreement primitives with the keys provided by quantum cryptography. Confidentiality and authentication is achieved by conventional VPN by making use of both public key and symmetric cryptography. Adding to the properties of conventional VPN and making it more secure, the DARPA-QKD secured network is fully compatible with conventional Internet hosts, routers, firewalls, and so forth.

E. *MagiQ Technologies*
It is one of the technology start-up companies that is working on developing quantum cryptographic solutions. Currently this company is targeting the financial services industry along with academic and government labs. MagiQ works with the philosophy that quantum cryptography is a complement to the current cryptographic algorithm and not a replacement to it. The quantum key distribution hardware box provided by MagiQ comprises a 40 pound chassis that is mountable in a 19 inch rack. The unit also includes a photon transmitter and receiver, electronics and software required for quantum key distribution. This unit is intended to change randomly generated keys once a second to prevent unauthorized access to data traveling over fiber optic lines.

VIII. CONCLUSION

We currently live in an information age which is the classical information age. We have done really well in order to transmit classic streams of ones and zeroes around the world but since last decade there has been substantial advancement in the field of quantum computers which leads to quantum cryptography and quantum internet. But still there are challenges ahead before quantum information theory that need to be worked upon and develop further. This includes developing more advanced hardware to achieve higher quality and longer distances for quantum key exchange and storing

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10570

any delicate quantum state for any length of time is hard which is the key feature on which quantum internet is based upon.

However, due to advancement in computer processing power which lead to a threat to the current cryptographic system will remain a motivating factor in the continued research and development of quantum information theory. If quantum computers really exist at some point we can use a post cryptographic algorithm until we develop a working quantum internet to protect us from black hat quantum hackers. But this doesn't mean someday someone will not come out with an idea which could destroy the post quantum cryptographic method. That is the reason,QKD sounds more promising as it is really hard to decode and makes eavesdropping almost impossible. even security agencies might have problems breaking these cryptosystems.

So. If someday quantum computers turn out to eventually meet even some of its expectations we will be able to build the quantum age which will have revolutionary effects in all of our lives. We will also be able to build the next generation of cryptographic protocols, distributed quantum computers, as well as achieve new level of development in quantum simulations which can provide new insight on protein that might revolutionize medicine, science or the new level of achievements of atomic clock synchronization and extreme precision in our interferometric telescope.

To sum it up, a properly implemented quantum network ensures secure and fast communication in contrast to classical cryptographic systems but research is needed in this field to make it a reality in the upcoming future.

REFERENCES

[1]. H. J. Kimble, "The Quantum Internet", June 2008
[2]. Bing Qi, Li Qian, Hoi-Kwong Lo, "A brief introduction of quantum cryptography for engineers", Research Gate Feb 2010
[3]. Chip Elliot, Dr. David Pearson, Dr. Gregory Troxel, "Quantum Cryptography in Practice", May 2003
[4]. Norbert Lutkenhaus, "Quantum Cryptography", March 2006
[5]. Alexandru Paler, Simon J. Devitt, "An Introduction into Fault-tolerant Quantum Computing", June 2007
[6]. Bochen Tan, Jason Cong, "Optimal Layout Synthesis for Quantum Computing", November 2020
[7]. Mario Piattini, Guido Peterssen, Ricardo Pérez-Castillo, "Quantum Computing: A New Software Engineering Golden Age", ACM SIGSOFT Software Engineering Newsletter, July 2020
[8]. Adrien Suau, Gabriel Staffelbach, Henri Calandra, "Practical Quantum Computing: Solving the Wave Equation Using a Quantum Approach"
[9]. Vadim Makarov, "Quantum cryptography and quantum cryptanalysis", March 2007
[10]. Alán Aspuru-Guzik, Wim van Dam, Edward Farhi, Frank Gaitan, Travis Humble, Stephen Jordan, Andrew Landahl, Peter Love, Robert Lucas, John Preskill, Richard Muller, Krysta Svore, Nathan Wiebe, Carl Williams, "ASCR Report on Quantum Computing for Science"
[11]. C.H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, December 1984, pp 175-179. Artur Eckert , Physical Review Letters 67, p. 661 (1991)
[12]. Margaret Martonosi and Martin Roetteler, "Next Steps in Quantum Computing: Computer Science's Role", November 2018, Computing Community Consortium
[13]. J. Aditya, P. Shankar Rao, "Quantum Cryptography", Andhra University
[14]. Mihir Pant, Hari Krovi, Don Towsley, Leandros Tassiulas, Liang Jiang, Prithwish Basu, Dirk Englund, Saikat Guha, "Routing entanglement in the quantum internet", Nature Partner Journals, March 2019