Quantum Internet: Realization and Security

Shakir Sajad
College Freshman, School: Candid Higher Secondary School, Nowgam, Kashmir, India

***Abstract*- The Quantum Internet [5] is the biggest and another surprising advancement of Quantum Mechanics [6], and would deal not only with crucial things of today's world, but provides a complete solution to the theory of Cryptography. It is not of novel science, rather an old one [1]. In Information theory communication is defined as message transfer between two parties and in basic definitions of artificial intelligence, if a system is misunderstood by a human to distinguish from a machine or a human, then the system is intelligent and can break on secure communication. In this paper, I shed light on how a perfectly fit system can be realized using Quantum Computer on Quantum Internet and providing a secure communication between two parties.**

***Index terms*- Quantum Computing, Quantum Internet, Quantum Algorithm, Entanglement, Quantum network, Cryptography, Qunatum Channel**

I.INTRODUCTION

Today, the world of Quantum Computer is receiving a tremendous amount of research and development. Potentially, a quantum computer can tackle classes of problems that choke conventional machines, such as molecular and chemical reaction simulations [4], optimization in manufacturing and supply chains, financial modeling, machine learning and enhanced security.

And, after the realization that quantum internet is theoretically possible, scientists left no stone unturned on putting forth every model that can describe working of quantum internet.

In classical computation, communication works between two or more parties by set of rules – Cryptography. Various algorithms are put to labor and communication is secured from eavesdrop. Sharing public and private keys is the basis of modern internet and they rely on mathematical models which are not very perfect at being complete. With today's power of processors, if a simple screen lock is to be broke by a computer, it would take 20 million years to break it.

That is very huge timeframe.

It might be very vague, because the source and value of information may expire in that timeframe. But, with the help of quantum computers and heavenly powers of calculations they possess, it is approximated that same information will be exploited in few days.

This could lead to very chaotic situations in which very crucial Intel would be leaked. Nuclear launch codes, state secrets, national information, and many other valuable resources that big agencies and governments want to maintain as secret will all be leaked and made public.

All these and many other applications arise for the quantum internet to solve. Quantum internet promises a state of smooth coherence and redundant free data in a system.

II. BACKGROUND OF QUANTUM MECHANICS AND QUANTUM SYSTEM

In classical physics or Newtonian mechanics any particle with mass can be treated as point object lest its mass remains constant and doesn't change throughout the experiment.

After that we can calculate the momentum (p) and velocity (v) of the particle and use various experiments on the system using [eq 1.1].

$$p = \frac{m}{v} \qquad \text{eq 1.1}$$

We can see from [eq 1.1] that with increase of mass velocity increase and so dose mass on increase of velocity and that implies we can precisely measure the impact of mass or velocity change on a system.

Werner Heisenberg in a paper on Uncertainty principle underplayed a statement in which he addressed that more precisely position of some particle is determined, the less precisely its

momentum can be predicted from initial conditions, and vice versa.[2]
This is called Uncertainty principle and is governed by eq 1.2.

$$\sigma x.\sigma p \geq \frac{h}{4\pi} \quad \text{[eq 1.2]}$$

Erwin Schrödinger used [eq 1.2] the equation in his famous equations.
When solutions of those equations are solved we come to the concept of superposition principle and Quantum entanglement. The very concept is used in a quantum computer and in quantum internet to deliver and receive information.

II.2 Quantum Entanglement
Defined as spooky action at a distance by Einstein, entanglement is property of two particles – quantum particles. When two electrons are entangled [eq 1.3] then took to two extremes of universe, the information stored in one electron is equally distributed by other. Same is done with qubits.

$$|\psi\rangle = |0\rangle + e^{i\varphi} + |1\rangle \quad \text{eq 1.3}$$

When one qubit is entangled with other qubit we can perform a measurement. A measurement can be any question. So, if we say 'Are you red?' to a qubit, both of the qubits will answer yes or no at that instant, and leading to interpretation is called bell measurement.

III QUANTUM COMPUTER

In a classical computer, bits are used which store data as 0 or 1.
At any instant only one of these can be stored (0 or 1). With quantum computer, data is store on advanced version called QU-BIT. In qubit, we can store two values at an instant 0 and 1, much like two entangled paired electrons can store electron up and electron down spin. With this rate if data is store on a quantum computer, then 3 qubits can store eight values all at the same time – with classical computer storing only one of the eight values at a time. This amount is tremendous and with more and more qubits data capacity is increased exponentially [fig 1.1] [3].

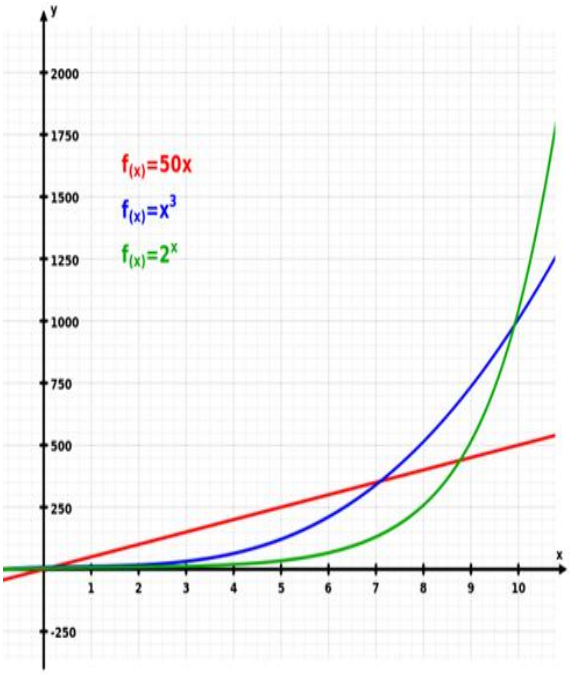

Fig1.1A description of exponential growth which a quantum computer follows. As f(x) = 2x

IV. PREDICTION ON QUANTUM INTERNET AND SECURITY

IV.1 Using Bell Measurement to Communicate /Quantum Channel
According to Bell measurement if two qubits are entangled and Alice has a qubit 'A' and bob has a qubit 'B' received via the quantum channel, then they can transfer messages with speed not more than speed of light.

Let's say Bill wants to send a message to Ted, than that message will be stored as the state of a third qubit, named qubit 'C'. Now, to send the message bill performs a particular type of measurement on his qubit via Bell Measurement. Performing the measurement simultaneously on A and C entangles them and breaks the entanglement with B [fig 1.2].
At this stage the information is completely sent to qubit B. Although, it is just a one bit of information, increasing the number of qubits will increase the size of information

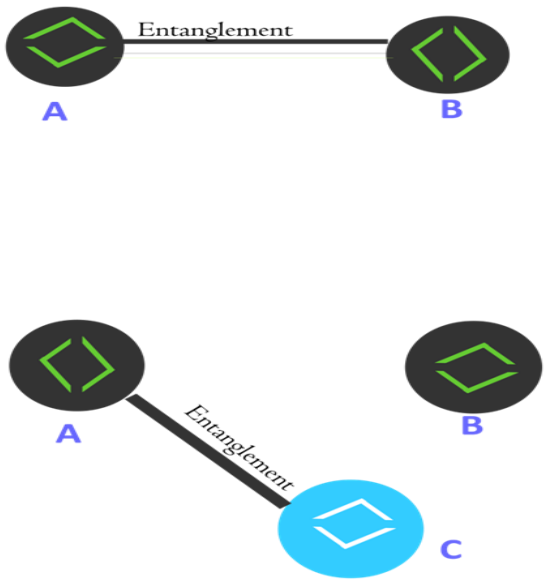

Fig 1.2

When qubit A is entangled with qubit C, old entanglement breaks and qubit B has state as of new qubit C's prior state.

This information is sent through quantum channel and is so secure that nothing can break it when combined with a quantum key distribution protocol. In classical cryptography when message is sent from say Bob to Alice, eavesdrop can break the classical channel of message and read the message before it is sent to Alice, without letting them know. However, in quantum cryptography this is not the case because of another weird rule of quantum mechanics. The rule says, "When you measure something like an electron's spin, the act of taking the measurement changes some of the electron's properties."

So if Alice sends a key to Bob and in any way an eavesdropper (anonymous) tries to read break in , both Alice and Bob would know that they channel has been compromised and that their conversation is no more secure, they will no more communicate on that channel and thus their conversation and secrets will not be compromised.

IV.2 Systematic Approach

In theory, a quantum system is predicted which works on normative algorithm to produce results of above findings. This quantum system will work on existing fiber optic cable because the network is already huge and we would like to take advantage of it

At the beginning only few nodes [fig 1.3] could be connected till the network is workable, as in the case of ARPANET.

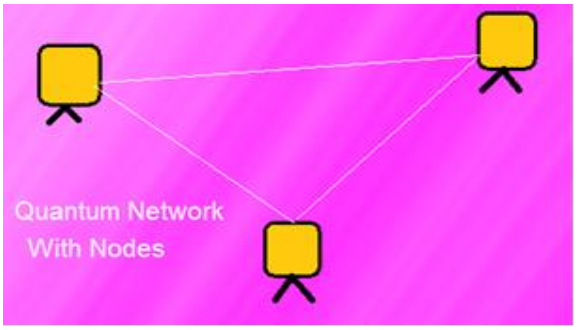

Fig 1.3 Few nodes connected to an early network.

IV.2.1 Existing Research on System

Massive models have been put forth to predict a system to work for this concept. Most of them are based upon a new quantum network, but only few are based on fiber optic cable as it very hard to keep up with photons – as of their wavelengths and fragile nature. Even the materials that are compatible with those cables can store quantum information for only a small fraction of second.

As a solution to this problem Australian team found a way to lengthen that time.

IV.2.2A Model

Using two quantum computers as two nodes can be made possible if quantum network is taken in place. Via that network we can create a channel to link two systems and entanglement can work on qubits.

V. NORMATIVE ALGORITHM

As Shor's algorithm [7], this quantum algorithm may be able to run on any quantum computer and the quantum network can be channeled with it.

Information exchange between two parties will take place before a handshake protocol takes place.

For a safe exchange, the system will check for eavesdrop and return values as per the presence of eve. If the channel is clear QUBITS will be entangled and information exchange will start.

V.2 Step Wise Algorithm

>Start

>Entangle Two QUBITS

>Open New Quantum Channel

>QUBIT share agreement
>Handshake Protocol Between Two Parties
>Agreement Of Protocol
>Alert To System For Start
>If protocol breaks through channel alert for eavesdrop
>Alert to both parties for an eavesdrop
>End messages
>Else continue
>Entangle pairs for message exchange
>End process

VI. CONCLUSIONS

By use of quantum internet and rules of quantum mechanics, a system is proposed which creates a quantum cryptographic version of classical information exchange system.
This project is an outstanding part of research and could benefit the huge brain of information theory and quantum computation.
I do look forward to contribute to such an exciting research area, which could pave the way for the next possible version of the internet such as Arpanet paved a way for today's internet and possibly WWW.

VII. ABBREVIATIONS

The following are the abbreviations used:
QUBIT: Quantum Bit
WWW: World Wide Web
ARPANET: Advanced Research Projects Agency Network.

REFERENCES

[1] R.P. Feynman. 1982. Simulating physics with computers. International Journal of Theoretical Physics 21, 6-7 (1982), 467 – 488.
[2] https://en.m.wikipedia.org/wik/Uncertainity>principle
[3] https://commons.m.wikimedia.org/wiki/File:Exponential.svg#mw-jumo-to-license
[4] K. Bourzac. 2017. 4 tough chemistry problems that quantum computers will solve [News]. IEEE Spectrum 54, 11 (November 2017), 7–9.
[5] D. Castelvecchi. 2018. The quantum internet has arrived (and it hasn't). Nature 554 (Feb. 2018), 289–292.
[6] Stefano Pirandola and Samuel L. Braunstein. 2016. Physics: Unite to build a quantum Internet. Nature 532, 7598 (Apr. 2016), 169–171.
[7] P. W. Shor. 1994. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE, 124–134.