QUANTUM COMPUTING-A Door To An Invincible Crypt

A Review paper on Basics of Quantum computing.

Chriss Philip Saji
Dept. of CSE
MBCCET Peermade
Kerala, India
chrissattasseril16@gmail.com

***Abstract*- Privacy, a word used to convey a sense of safety and security has been reduced in all its rightful meanings into something fancy; a fancy that has come to be enjoyed blindly and claimed to be provided to everyone equally and fairly while, it is all just a puppet show by the masters hidden behind the well-built walls masqueraded as saviours. Souls aware of the recent happenings of this world would be well informed about the price whistle-blowers and journalists pay for the work they do to shine some light on the dangerously dark world corrupt leaders have built. Providing an umbrella of employment to individuals from both the department of physics and computer science it has created a marvel of conglomerate, wielding pamphlets of "promise-of-an-easy-era" across the world, while the technology works tirelessly through complex networks of qubit handling machines to make advancements in the field of medicine, defence, engineering, construction, space and what not.**

Keywords- Qubits, Quantum teleportation, privacy, security.

I. INTRODUCTION

Quantum, just as complex as it sounds is in fact really a magic that has managed to lift scientists, physicists and computer enthusiasts in its magic whirl through all its toughness and teleport them to some magical la-la-land promising each one a name in the inscribed foundation of the coming era. The domain even though is in its infancy stage; owing to all the revolutionising opportunities available, promises to convert the veiled complexity of this world into something more manageable and light-weighted for human minds to carry while going around with their chores.

Privacy, a word used to convey a sense of safety and security has been reduced in all its rightful meanings into something fancy; a fancy that has come to be enjoyed blindly and claimed to be provided to everyone equally and fairly while in reality, it's all just a puppet show by the masters hidden behind the well-built walls masqueraded as saviours. Souls aware of the recent happenings of this world would be well informed about the price whistle-blowers and journalists pay for the work they do to shine some light on the dangerously dark world corrupt leaders have built. Just as Julian Assange bravely said: "Cryptography is the essential building block of independence for organisations on the internet, just like armies are the essential building blocks of states because otherwise one state just takes over another" while being carried away to be prosecuted for his brave deed of exposing corruption and illegalities of various big players in the world.

The more you think about it, the more satisfying it feels to understand that domains like blockchain and quantum cryptography have chiselled out paths for many of such pressing problems through safe channels like CIVIL DApp and Quantum communication. These new fields are also being immensely explored by defence forces of various countries to make their communications secure and encrypted enough to talk fearlessly to exchange vital info across defence lines.

Though being in its infancy stage, it has proved to be a game changer in the industry. Providing an umbrella of employment to individuals from both the department of physics and computer science it has created a marvel of conglomerate, wielding pamphlets of "promise-of-an-easy-era"

across the world, while the technology works tirelessly through complex networks of qubit handling machines to make advancements in the field of medicine, defence, engineering, construction, space and what not.

Causa-

I developed a keen interest in the field while exploring my options as a CSE student who was interested in both quantum physics and the security aspect of this engineering field while also following a woke mind in the social world and noticing the dangerous aura we all live in. The potentiality of this topic has come to amaze me.

While still unaware of many of its concepts, I hereby begin my journey to work towards a future me, a me skilled in at least two steps more from where I start today.

II. QUANTA, THE TRUE MESSIAH

The true soul of quantum information is rightly attributed to Qubit. A replacement for the 0's and 1's of classical computing. Just as bits are responsible for every process in the "fetch-decode-execute" -cycle, the transfer of qubits across various quantum states makes quantum communication a reality. These quantum-mechanical entities can exist in more than one state at a particular time gap. This became true in the guidance of the superposition principle, which implies that they can be in a combination of more than one state represented by |0› and|1› respectively at the same time. There is 2-D vector space known as Hilbert space which forms the basis for the representation of qubits. The two basic vectors |0› and|1› are perpendicular to each other and form the Bloch sphere, in which every vector present is in a valid quantum state. One of the main fundamentals is Quantum entanglement which says that if two Quantum states are satisfactorily bonded with each other enough then their separation becomes impossible. E.g.- Consider two friends, if each one is considered to be a qubit in a vector space of Hilbert space and they are said to be Quantum entangled then their separation becomes an impossible thing even if you take the other one hundreds of kilometres away. This has enabled the researchers to solve the mysteries of transferring qubits across states without sending them across. It does it in a way that creates an illusion that nothing happened, a real practice of magic. This is done using three parties say A, B, C or namely Alice, Bob, and Charlie, in which Alice and Bob remain in their exact quantum states while Charlie gets entangled with Alice and transfers the measurement results to the receiver over regular communication channels; the receiver then imitates the condition of the sender to weave the magic. Various quantum algorithms using these principles are used to iterate and solve complex problems.

III.SHOR'S ALGORITHM

One of the basic underlying roots of almost all bank transactions, virtual private networks, message transfers etc are all based on Rivest-Shamir-Adleman or RSA cryptographic algorithm. This algorithm uses the concept of factorization of very large prime numbers to generate keys. The bigger the value of prime numbers, the tougher it would be to find the factors which hold the key to RSA encryption. The encryption works by generating two keys: a private and a public one. The public one is held by the sender while the receiver holds the private one. The message is broken down into blocks and then mathematically worked with the public key to form large complex numbers which can be decrypted by only the private keys. Since breaking down of RSA key of current standards(2048-bit) would take hundreds of years, it remains a safe protocol for encryption today. however, quantum computers could easily break these down in mere hours using quantum parallelism, another merit of Quantum computing which allows them to work out calculations simultaneously. This was known when Peter Shor discovered Shor's algorithm in 1994, which

became famous for its capability to break down large numbers into factors. Working: first, select a random number 'a' between 2 and complex number, N. Then find out the greatest common divisor of N using a and if the value is not equal to1 then the gcd value is a nontrivial factor of N (a solution in which the value of at least one variable of the equation is not equal to zero), else a quantum Fourier transform-the soul of this algorithm is utilised to find the factors and the order by first finding the period with help of the superposition principle. Lastly, if the GCD of the number, N and (a^{order}/2+1) is nontrivial, then the second factor is N/gcd-value and the step ends there, else start from the beginning. Confidence in the safety of our encryption can be ascertained by the fact that post-quantum-cryptography is being developed at a fast pace to counter Quantum attacks.

IV. GROVER'S ALGORITHM

Another famous algorithm developed was Grover's algorithm which is used to sort an unsorted data set in a time period of O(sqrt(N)) much faster than the traditional speed of classical computers(O(N)) where N is the size of the database. it searches through all possible inputs using an Oracle or a black box, an unknown entity represented by an unknown function in which strings are provided as inputs and outputs are single bits, used to determine the falsity of inputs. The algorithm works without any knowledge of how the box is working or what the function inside it is doing. This algorithm is believed to get through symmetric encryption keys easily. Hence, concerned parties were advised to double the lengths of the keys to prevent that. The association of machine learning with quantum computing is another major noticeable field that is currently being worked upon. Utilising quantum parallelism techniques they have managed to create much more efficient and powerful algorithms by training on large datasets parallelly.

Despite all these amazing capabilities that these marvels seem to display, some problems seem to be bothering them in a big way. Noise-one of its biggest problems is a term to refer to unwanted interactions between the outside universe and the quantum system. These quantum systems are very much sensitive and as the size of these grow-depending on the number of qubits they are working on, they become more and more sensitive to all kinds of outside disturbances be it of any kind thermal, electric, sonic etc. These noises could lead to errors in computation due to changes in the state of quanta. Storing it in temperatures nearing absolute zero-using cryogenic cooling or using quantum error correction codes are some of the ways in which these systems are made to do the work upright. Quantum error correction is a set of techniques practised by encoding the current system in a larger quantum system to correct emerging errors. Ancilla qubits, the ones used to refer to the extra qubits present in the larger quantum system, have the unique property of being affected by any error that occurs. This information is then used to proceed with a set of quantum operations to reverse the errors in computation. Fault-tolerant-quantum-computing is just another fancy name to encapsulate the idea of quantum error correcting codes to achieve and utilise their full potential.

All these merit terms collectively point towards a single term covering them all – The Quantum supremacy. It simply follows the literal meaning and says that these systems can outperform all the classical and super-computers in all the ways possible. For instance, the application of Shor's algorithm is just the tip of the iceberg. In 2019, Google performed a specific problem in their 53-qubit quantum computer in just 200 seconds, a task they claimed would take the current supercomputers thousands of years to solve.

V.QKD-QUANTUM KEY DISTRIBUTION

A very interesting topic as it is, it is equally as much crucial and necessary. It is one among the various protocols used in quantum cryptography, a sublet of cryptography which uses the principles of quantum mechanics to create secure communication channels between interested parties, a vital necessity along defence lines. This mechanism promises to find any interception that is made. Qkd can be done through different types of media such as fibre optics, free space, and even satellite-based communications. Its working goes as follows: Let Alice and Bob be the interested parties. Alice prepares the quanta in some quantum states which are mutually perpendicular to each other and then sends these over one by one to bob over the communication channel. Bob then polarizes the received photons in a way that may be either similar or different to that of Alice's polarization and then the difference between the two is measured using a detector, if the error rate comes out to be high, the protocol is dropped. They then use the remaining photons to make a secret key that can be used for further communications which is completely free from any types of eavesdropping. Many types of privacy amplification protocols can also be engaged to make security stronger. Quantum cryptography although providing a very high detail of security, needs to overcome some challenges like the speed of protocols or the distance over which they can be transferred to make this prove a messiah of the industry.

VI.REFERENCES

1. Basic to advanced key point list of quantum computing:https://www.ibm.com/blogs/research/2019/07/quantum-computing-terms/
2. An introduction to Quantum computing for non-physicist's: https://dl.acm.org/doi/abs/10.1145/367701.367709
3. Quantum state in detail: https://en.wikipedia.org/wiki/Quantum_state
4. Two-dimensional Hilbert space: https://en.wikipedia.org/wiki/Hilbert_space#Two-dimensional_Hilbert_space
5. Quantum entanglement: https://en.wikipedia.org/wiki/Quantum_entanglement
6. Superdense coding: https://en.wikipedia.org/wiki/Superdense_coding
7. Quantum teleportation: https://en.wikipedia.org/wiki/Quantum_teleportation
8. RSA: https://en.wikipedia.org/wiki/RSA_(cryptosystem)
9. Post-quantum cryptography: https://en.wikipedia.org/wiki/Post-quantum_cryptography
10. Grover's algorithm: https://en.wikipedia.org/wiki/Grover%27s_algorithm
11. Quantum error correction: https://en.wikipedia.org/wiki/Quantum_error_correction
12. Quantum Fourier transform: https://en.wikipedia.org/wiki/Quantum_Fourier_transform
13. "Quantum Key Distribution" by NIST: https://www.nist.gov/programs-projects/quantum-key-distribution
14. "Quantum Cryptography" by Stanford Encyclopaedia of Philosophy:https://plato.stanford.edu/entries/qt-quantum-cryptography/
15. "Quantum Key Distribution" by IBM: https://www.ibm.com/topics/quantum-key-distribution
16. "An Introduction to Quantum Cryptography" by Phys.org: https://phys.org/news/2019-08-introduction-quantum-cryptography.html
17. "Quantum cryptography: A beginner's guide" by ZDNet: https://www.zdnet.com/article/quantum-cryptography-a-beginners-guide/
18. Quantum Computing in general: chat.openai.com

Under the guidance of
Prof. Ushus Maria Joseph
Dept. of CSE, MBCCET Peermade, Kerala, India

Volume 11, Issue 04 Published by, www.ijert.org ISSN: 2278-0181