International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Are Quantum Computers the Future of Fast Computation

Naresh Sambhaji Ghorad

Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India
ghoradnaresh[at]gmail.com

Abstract: ***Quantum computing has become a hot topic in recent years. The device that used for quantum computing is Quantum computer. Quantum computers are machines that use the properties of quantum physics to store data and perform computations. This can be extremely advantageous for certain tasks where they could vastly outperform even our best supercomputers. Classical computers, which include smartphones and laptops, encode information in binary "bits" that can either be 0s or 1s. In a quantum computer, the basic unit of memory is a quantum bit or qubit. There has been some successful development of quantum computer technology, but a great deal of research and development remains to be done before quantum computers become viable as a mainstream technology, and there are arguments as to why this eventuality can never be achieved. The proposed research is focused on Cyber security-Will quantum Computing break the Cyber security?***

Keywords: Quantum computers, Supercomputers, Classical computers, Cyber security

1. Introduction

Quantum computing is a type of computation that harnesses the collective properties of quantum states, such as superposition, interference, and entanglement, to perform calculations. The devices that perform quantum computations are known as quantum computers. [1] They are believed to be able to solve certain computational problems, such as integer factorization (which underlies RSA encryption), substantially faster than classical computers. The study of quantum computing is a subfield of quantum information science. Expansion is expected in the next few years [when?] as the field shifts toward real-world use in pharmaceutical, data security and other applications. [2] Quantum computing began in 1980 when physicist Paul Benioff proposed a quantum mechanical model of the Turing machine. [3] Richard Feynman and Yuri Manin later suggested that a quantum computer had the potential to simulate things a classical computer could not feasibly do. [4] [5] In 1994, Peter Shor developed a quantum algorithm for factoring integers with the potential to decrypt RSA-encrypted communications. [6] Despite ongoing experimental progress since the late 1990s, most researchers believe that "fault-tolerant quantum computing [is] still a rather distant dream. [7] In recent years, investment in quantum computing research has increased in the public and private sectors. On 23 October 2019, Google AI, in partnership with the U. S. National Aeronautics and Space Administration (NASA), claimed to have performed a quantum computation that was infeasible on any classical computer, but whether this claim was or is still valid is a topic of active research. [8]

2. Quantum Superposition

Superposition is the term used to describe quantum state where particles can exist in multiple states at the same time, and which allows quantum computer to look at many different variables at the same time. A qubit (or quantum bit) is the quantum mechanical analogue of a classical bit. In classical computing the information is encoded in bits, where each bit can have the value zero or one. In quantum computing the information is encoded in qubits. A qubit is a two-level quantum system where the two basis qubit states are usually written as$|0\rangle$ and $|1\rangle$. A qubit can be in state$|0\rangle$, $|1\rangle$ or (unlike a classical bit) in a linear combination of both states. The name of this phenomenon is superposition.

Qubits can be in a superposition of both the basis states $|0\rangle$ and $|1\rangle$. When a qubit is measured (to be more precise: only observables can be measured), the qubit will collapse to one of its eigenstates and the measured value will reflect that state. For example, when a qubit is in a superposition state of equal weights, a measurement will make it collapse to one of its two basis states $|0\rangle$ and $|1\rangle$ with an equal probability of 50%. $|0\rangle$ is the state that when measured, and therefore collapsed, will always give the result 0. Similarly, $|1\rangle$ will always convert to 1.

Quantum superposition is fundamentally different from superposing classical waves. A quantum computer consisting of n qubits can exist in a superposition of 2n states: from$|000\ldots0\rangle$ to$|111\ldots1\rangle$. In contrast, playing n musical sounds with all different frequencies, can only give a superposition of n frequencies. Adding classical waves scales linear, where the superposition of quantum states is exponential.

3. Quantum Computers vs Classical Computers

Let's explore some of the major differences between quantum computers and classical computers.

- **Information processing**: While conventional computers rely on transistors, which represent the binaries *0* or *1*, quantum computers use qubits. Qubits follow the superposition principle and can represent both *0* and *1* at the same time.
- **Power**: The power of quantum computers grows exponentially in proportion to the number of qubits linked together. This is different from what happens in

classical computing. The power of a classical computer increases linearly with the number of transistors.

- **Applications**: Quantum computers are better suited for complex tasks, such as optimization problems, data analysis and processing, and simulations. Classical computers are better for our everyday processing needs.
- **Building blocks**: Superconducting Quantum Interface Devices (SQUID) or quantum transistors are the basic building blocks of quantum computers. Classical computers use CMOS transistors.
- **Data processing**: In quantum computing, data processing occurs in the Quantum Processing Unit (QPU), which consists of interconnected qubits. In classical computing, data processing occurs in the Central Processing Unit (CPU), which consists of the Arithmetic and Logic Unit (ALU, processor registers, and a control unit.
- **Information representation**: Classical computers use bits, while quantum computers use qubits.
- **Speed**: Quantum computers can solve certain problems hundreds of millions of times faster than traditional computers. For example, in 2019, Google's quantum computer did a calculation in less than four minutes that would take the world's most powerful supercomputer 10, 000 years to do.

4. Quantum Computing vs Cyber Security

Tomorrow's quantum computers are expected to be millions of times faster than the devices that we used now a days. So, when these powerful computers are actually built, there is a good chance that your data will be hacked.

Suppose you have account in a bank. Assume that only you and your bank can access your information, you have strong password and you are using two-factor authentication. You know that bank has solid security system; hence you are confident that no one else can see Change your sensitive data.

In future you log into your account, and you see that your savings have been transferred elsewhere. How it become possible? What happened to your password, banks security system, Two-factor authentication?

This happened because hackers use quantum computer. Because of quantum computer's speed hackers can easily break security algorithm. This threat cold affect everything like Bank accounts, military communications, Secret records, our valuable data and so on.

5. Quantum Cryptography

Quantum cryptography is a technology that uses quantum physics to secure the distribution of symmetric encryption keys. Quantum cryptography algorithms have the potential to crack traditional cryptography keys, which are currently too complex for classical computers to crack. While engineers race to develop the first advanced quantum computer, cyber security experts are racing to roll out a new form of cryptography that would defend against quantum hacks. This is known as post-quantum cryptography or PQC.

In cryptography, post-quantum cryptography (sometimes referred to as quantum-proof, quantum-safe or quantum-resistant) refers to cryptographic algorithms (usually public-key algorithms) that are thought to be secure against a cryptanalytic attack by a quantum computer. Experts are currently developing PQC solutions, but these will need to be standardized and widely adopted. That could take years or even decades. "Post-quantum cryptography is the best solution, " said Vermeer. "It's just a matter of getting it done in time. "

6. Google's Quantum Computer

Google has officially announced that its achieved quantum supremacy in a new article published in the scientific journal Nature. Google says that its 54-qubit Sycamore processor was able to perform a calculation in 200 seconds that would have taken the world's most powerful supercomputer 10, 000 years. That would mean the calculation, which involved generated random numbers, is essentially impossible on a traditional, non-quantum computer. This extra processing power could be useful to simulate molecules, and hence nature, accurately, Google says. This might help us design better batteries, creating more carbon-efficient fertilizer, or develop more targeted medicines, because a quantum computer could run simulations before a company invests in building real-world prototypes. Google also expects quantum computing to have big benefits for AI development.

7. Findings

- Quantum computing can change our computing world.
- Very less people are aware about this computer.
- Peoples are willing to use this quantum computer.
- Quantum computers are the future of fast computation.
- Quantum cryptography can break traditional cryptography.
- But there is a solution on it, PQC (Post Quantum Cryptography).

8. Conclusion

In this paper I have reviewed the principles, algorithms and cyber security of quantum computing. The foundations of the subject of quantum computation have become well established, but everything else required for its future growth is under exploration. Quantum computers have the potential to revolutionize computation by making certain types of classically intractable problems solvable.

Quantum computers have potential to benefit society in various ways. Quantum computers can solve problems that are impossible or would take a traditional computer an impractical amount of time (a billion years) to solve. Quantum computers have potential to change our world of computing.

They have some drawbacks also. Quantum cryptography can break traditional Cryptography. Hackers can use quantum computers that may lead to the cyber attacks.

While engineers race to develop the first advanced quantum computer, cyber security experts are racing to roll out a new form of cryptography that would defend against quantum hacks. This is known as post-quantum cryptography, or PQC. PQC is the best solution.

9. Acknowledgement

I would like to extend our heartiest thanks with a deep sense of gratitude and respect to all those who provides me immense help and guidance during my period.

I would like to thank my teacher **Prof. Gauri Ansurkar** ma'am for providing a vision about the research paper. I have been greatly benefited from their regular critical reviews and inspiration throughout my work. I am grateful to them for their guidance, encouragement, understanding and insightful support in this research paper.

Finally, I must express my very profound gratitude to my parents and to my friends for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

References

[1] The National Academies of Sciences, Engineering, and Medicine (2019). Grumbling, Emily; Horowitz, Mark (eds.). Quantum Computing: Progress and Prospects (2018). Washington, DC: National Academies Press
[2] "Scopus for Corporate Research & Development"
[3] Benioff, Paul (1980). "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines". Journal of Statistical Physics.22 (5): 563–591.
[4] Feynman, Richard (June 1982). "Simulating Physics with Computers" (PDF). International Journal of Theoretical Physics.21 (6/7): 467–488.
[5] Manin, Yu. I. (1980). Vychislimoeinevychislimoe [Computable and Noncomputable] (in Russian). Sov. Radio. pp.13–15. Archived from the original on 10 May 2013. Retrieved 4 March 2013.
[6] Mermin, David (28 March 2006). "Breaking RSA Encryption with a Quantum Computer: Shor's Factoring Algorithm" (PDF). Physics 481-681 Lecture Notes. Cornell University. Archived from the original (PDF) on 15 November 2012.
[7] Preskill, John (2018). "Quantum Computing in the NISQ era and beyond". Quantum.2: 79. arXiv
[8] "On 'Quantum Supremacy'". IBM Research Blog.22 October 2019. Retrieved 9 February 2021.
[9] https://www.newscientist.com/question/what-is-a-quantum-computer/#ixzz79BabR5Vg
[10] https://en. m. wikipedia.org/wiki/Quantum_computing
[11] https://www.google.com/amp/s/www.theverge.com/platform/amp/2021/5/19/22443453/google-quantum-computer-2029-decade-commercial-useful-qubits-quantum-transistor
[12] https://www.quantum-inspire.com/kbase/superposition-and-entanglement/
[13] https://www.rand.org/blog/articles/2020/04/quantum-computers-will-break-the-internet-but-only-if-we-let-them.html