Grenze International Journal of Engineering and Technology, June Issue

Quantum Computing Demystified: Concepts, Algorithms, and Implications for Classical Computer Science

Priyanshi Saxena[1], Roshan Lal[2] and Nidhi Kaushik[3]
[1-2]CSE Department, ASET, Amity University, Noida, Uttar Pradesh, India.
Email: km.saxena1@s.amity.edu, chhokar@amity.edu
[3]IT Department, Amity School of Law, Amity University, Noida, Uttar Pradesh, India
Email: nkaushik2@amity.edu

***Abstract*— Quantum computing is a technology that is built around several theoretical principles. quantum mechanics quantum superposition, quantum entangler, quantum qubits. It is in this paper that I will give a brief. also brief discussion of the fundamentals of quantum measurement and the working of quantum gates. as descriptions and illustrations of some of the famed algorithms like Shor algorithm and the algorithms by Grover which are exponentially better than the classical ones. Other than the speed benefits of quantum computing, the quantum computing implications go beyond speed. much more than the speed of calculations. The quantum computers will have an influence in the way we design and develop. computer algorithms and also influence the way we lock our information and guard it against. unauthorized access. Quantum computing will have the possibility of hybridization in the future. with quantum and classical computing. The current research and development. quantum computing has been the focus of research that still presents an abundance of challenges and hurdles, however. the advantages and opportunities that this technology offers are much greater in comparison to the disadvantages. This paper will also strive to shed light on and describe the principles of quantum computing and the potential impact it. that will be the case of all computer scientists today and tomorrow.**

***Keywords*— Quantum Computing, Qubits, Quantum Algorithms, Cryptography, Classical Computation.**

I. INTRODUCTION

Unlike what we have in classical computers with the number system of 0 and 1, quantum computing employs the use of qubits. The unit of information in quantum computing is known as qubits and they possess special abilities as they exploit the power of superposition, entanglement, and quantum interference. Qubits enable novel ways of information processing which cannot be done with any kind of traditional computers (see Nielsen and Chuang 2010). Feynman suggested a quantum computer to simulate a quantum system since he was aware that there would be constraints to the capabilities of classical computers to simulate a quantum system. Theoretical work has since advanced to practice, with Google in 2019 announcing that it has achieved quantum supremacy by successfully implementing a quantum computer to solve a problem beyond the bounds of the fastest classical supercomputers [1] (The qubit is the basic unit of quantum computing).

Grenze ID: 01.GIJET.12.2.170_20

Every quantum computer is constructed using quantum bits (qubits) and quantum physics of a qubit is what provides a quantum computer with its special properties.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

where α and β are complex amplitudes satisfying $|\alpha|^2 + |\beta|^2 = 1$ [3]

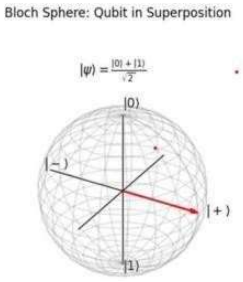

Fig 1. Bloch Sphere Representation of a Qubit in Superposition

Quantum algorithms demonstrate the potential of quantum computing. Shor's 1994 algorithm, for instance, shows how quickly to factor large integers compared to classical techniques. That is critical for asymmetric cryptography RSA [4] and similar systems. Grover's 1996 algorithm provides a quadratic speedup for unstructured searches and will be valuable in many applications, including optimization and machine learning. Both of these quantum algorithms involve a quantum Fourier transform and its associated operations.

$$QF\ T|j\rangle = 1\ \sqrt{}\ N\ N\ X{-}1\ k{=}0\ e\ 2\pi ijk/N\ |k\rangle \quad (2)$$

Although some systems are able to transmute quantum states with great success [3], we must not forget that present-day noisy intermediate-scale quantum (NISQ) devices leave a lot to be desired. With the current problems of decoherence and an abundance of errors, strong error-correction methods such as surface codes [5, 6] are often required just to keep things going in the right direction. Additionally, quantum computing is disrupting the computer science field in a major way. Several areas including cryptography are being significantly impacted. Shor's Algorithm presents a major threat to all of the current encryption schemes in use today therefore, NIST has stepped in to establish post-quantum cryptography standards to combat this threat [7, 8]Individuals currently working in computer science will likely need to develop new skill sets, including working with programming languages designed for quantum computing platforms (e.g., Qiskit, Cirq) and will need to rethink the boundaries between complexity classes such as BQP, P, and NP [9].

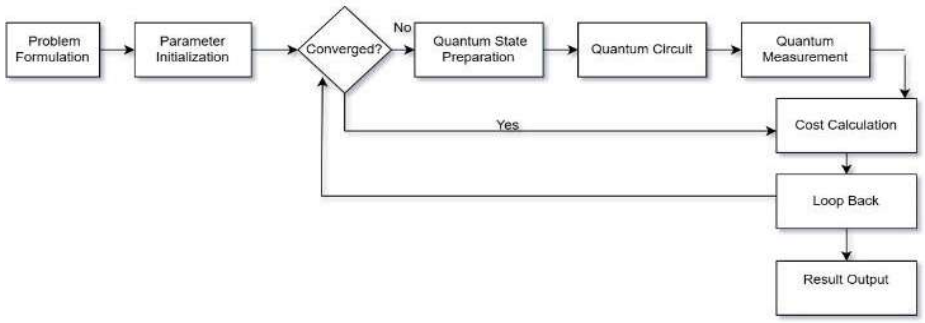

Fig 2. Hybrid Quantum-Classical Workflow

II. Literature Review

At this time, Quantum Computers are not going to take the place of your normal computer. They perform best at performing specific tasks at an expert level. The combination of quantum computer and computer science appears to be a new area of technology that will allow Quantum Computers to deal with issues that regular computers cannot. In 1982, Richard Feynman stated that if you want to simulate the uniqueness of quantum systems, you will need a Quantum Machine. This statement provided the foundation for the development of Quantum Computing. Later, Nielsen and Chuang developed some of the initial concepts of Quantum Computing

in their book, Quantum Computation and Quantum Information. They were the ones who created the fundamental theory of Quantum Computing. Some of the original concepts that were developed in this book have stood the test of time and are still considered essential in the current understanding of quantum computing. This book lays the foundations for all of the modern quantum computing concepts that are still in use today: qubit, superposition, entanglement, quantum gate. With these concepts, Quantum Computers can process the same amount of information concurrently with many different states of use at the same time. Therefore, this is what distinguishes Quantum Computers from earlier classical computers; they execute tasks and processes in an entirely different manner and manage multiple possible states simultaneously. Research has been greatly influenced over the years by developments in quantum algorithms. To illustrate, Shor's 1994 paper about an algorithm that could factor integers exponentially faster than a classical computer opened up an avenue of post-quantum cryptographic research [7] at the 35th Annual Symposium on Foundations of Computer Science. In addition to Shor, Grover presented an algorithm that provides a quadratically improved solution to unstructured search (i.e., optimization problems and searching through large databases) at the ACM Symposium on Theory of Computing, continuing the trend of creating new research areas in quantum computing. More recently, research opportunities have opened up in the area of hybrid quantum-classical algorithms, such as the Variational Quantum Eigen solver (VQE) and Quantum Approximate Optimal Algorithm (QAOA). These algorithms appear to be the best candidates for near-term implementation on NISQ devices, which were discussed further by McClean et al [12]Preskill made a statement in 2018 introducing the term "NISQ"to refer to the stage we are at now where we have noisy, imperfect quantum computers with only a few qubits and limited by decoherence. Preskill envisioned a future where quantum computers work together with classical computers. In 2019, the Google research team and Arute made huge headlines when they claimed that they achieved "quantum supremacy" with their Sycamore chip. By 2022, NIST began to investigate new standards for post- quantum cryptography and published CRYSTALS-Kyber, among others, to ensure that they remain at the forefront. At the same time, Bauer and others have documented instances were quantum and classical computing work together within quantum chemistry. Or´us, in a review published in Nature Reviews Physics, shared another perspective; many classical algorithms were created using the concepts behind quantum ideas. The influence potentially runs in both directions. As of 2025, IBM has developed quantum computing systems with greater than one thousand physical qubits and Microsoft have developed quantum computers using topological qubits [13].

TABLE I: COMPARISON BETWEEN PREVIOUS RESEARCH PAPERS

Year	Authors	Ref No.	Objective	Approaches	Evaluation	Strength/Weaknes s
2019	Ante et al.	[1]	Demonstrate quantum supremacy	Programmable superconducting processor (Sycamore)	Task completion time vs. classical super computers	**Strength:** First experimental proof quantum advantage **Weakness:** Specialized task with no practical application
2020	Basar et al.	[2]	Advance quantum chemistry simulation	Hybrid quantum classical algorithms	Accuracy in molecular energy calculations	**Strength:** Enables practical NISQ applications **Weakness:** Limited to small molecules
1984	Bennett & Brassard	[3]	Secure quantum key distribution	BB84 protocol	Security against eavesdropping attacks	**Strength**: Information-theoretic security **Weakness**: Short distance transmission limitations
2017	Bernstein & Lange	[4]	Develop quantum resistant cryptography	Lattice-based cryptographic schemes	Security analysis under quantum attacks	**Strength: Standardized by NIST PQC Weakness: Larger key sizes than classical cryptography**
2019	Dyakono v	[5]	Critique quantum computing feasibility	Error rate modeling	Practical implementation challenges	**Strength: Highlights fundamental limitations Weakness: Underestimates error correction advances**
1935	Einstein et al.	[6]	Examine quantum entanglement	EPR paradox thought experiment	Completeness of quantum mechanics	**Strength: Founding theoretical basis Weakness: No implementation roadmap**
1982	Feynman	[7]	Simulate quantum physics	Quantum computer concept	Computational complexity reduction	**Strength: Founding theoretical basis Weakness: No implementation roadmap**

2012	Fowler et al.	[8]	Enable fault tolerant quantum computing	Surface code error correction	Error threshold analysis	**Strength: High fault-tolerance thresholds Weakness: High qubit overhead (1,000+ per logical qubit)**
2023	Gambetta	[9]	Scale quantum processors	IBM quantum roadmap (127—1,000+ qubits)	Qubit count and connectivity metrics	**Strength: Clear scalability path Weakness: Persistent high error rates**
1996	Grover	[10]	Accelerate unstructured search	Quantum amplitude amplification	Query complexity ($O(\sqrt{N})$ vs. classical $O(N)$)	**Strength: Qualitative speedup for optimization Weakness: No exponential advantage**

III. Review Methodology

A. Data Collection

In this composition, I used numerous sources thoroughly to give the complete picture of quantum computing how it pioneered the major principles and algorithms that are related to quantum computing and the impact it will have on traditional computer science. I would like to add some clarity to overcome different misunderstandings that were associated with this topic. several sources to have an understanding of the history of quantum computing. I have read across several scholarly works. databases such as Pegasus, ACM Digital Library and Google Scholar.

B. Selection Criteria

Famous seminal works, including the Shor algorithm (1994) and Grover algorithm (1996) of search, as well as others of choice. classical literature [3] and the emerging development [1], were carefully omitted in order to have a balanced emphasis between ancient works and modern trends. Peer-reviewed studies were chosen as a priority in the selection of literature. dealing with quantum computing, quantum algorithms and their impact on classical computational paradigms.

IV. Core Concept of Quantum Computing

A qubit is fundamentally different from a classical bit. While a classical bit can exist only in a single fixed state, either 0 or 1, a qubit can represent a combination of both states at the same time due to its quantum nature. Mathematically, a qubit's state looks like

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

where α and β are complex numbers and $|\alpha|^2 + |\beta|^2$ always adds up to 1.

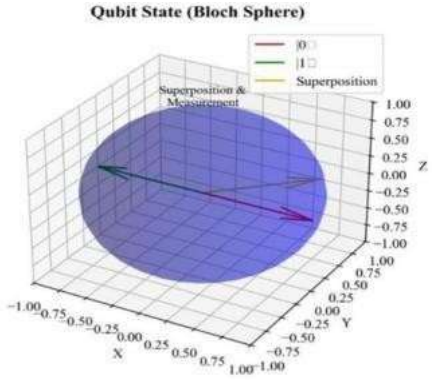

Fig 3. Bloch Sphere Representation of a Qubit State and Entanglement

A. Quantum Gates

These gates do all things in reversible operations. An example is that of the Hadamard gate. It throws a qubit into superposition. The CNOT gate That is how qubit entangle [3]. It is reversibility that is important here. In quantum it is always possible to undo the action and start computing over again. That is a huge contrast of how usually classical computing works.

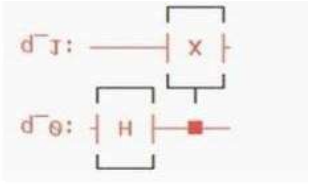

Fig. 4 Hadamard and CNOT Gate Circuit to Create Entanglement

B. Quantum Coherence and Noise

Qubits don't like noise. The slightest amount of it may disrupt the situation, leading to the collapse of their delicate quantum states and become ordinary, traditional states. This is referred to as a decoherence problem and is one of the largest headaches of those who make attempts.

V. QUANTUM ALGORITHMS

A. Shor's Algorithm (1994)

In 1994, Shor developed an algorithm that is capable of factoring large numbers much faster than we had previously done. This matters a great deal since RSA encryption the mechanism that makes most of our online conversation secure is based on the fact that it is difficult to factor these numbers. This is the way that the algorithm of Shor works: it combines regular and quantum computing to make factoring a far easier problem.
Process: First, any random number a is selected, making sure that its value is smaller than N. After that, a quantum register is created and it is set in such a way that it can represent all possible values of x at the same time.Next, modular exponentiation is carried out to calculate the value of the function f(x), which is defined as a raised to the power x modulo N.Once this step is completed, the Quantum Fourier Transform is applied to the quantum state in order to identify the period r.In the final step, classical mathematical computation is used to find the greatest common divisor of N and a^(r/2) + 1, which helps in determining the factors of N.

B. Grover's Algorithm (1996)

Grover's algorithm improves this process by increasing the likelihood of getting the correct result step by step. During each cycle, an oracle is applied to identify the required element. After that, a diffusion operation is performed to increase its probability compared to the remaining elements. With repeated iterations, the desired result becomes more noticeable, which allows the search to finish in much less time than traditional techniques.
Step-by-Step Process:

- Prep n qubits in a uniform superposition.
- Use the oracle to label the target state by changing the phase of the oracle.
- Use the diffusion operator to double the amplitude of the target.
- O(√ N) iterations, N = 2n, and then read out.

C. Quantum Fourier Transform (QFT)

QFT is basically the quantum version of the classical Fourier Transform, and it's a key part of algorithms like Shor's and quantum phase estimation [3]
Step-by-Step Process:

- Set qubits up on a computational basis state.
- Perform a series of controlled phase rotations according to qubit indices.
- Implement Hadamard gates on all qubits in order to achieve superposition.
- The terminal state bears the Fourier transform.

D. Variational Quantum Algorithms (e.g., VQE, QAOA)

As a goal of noisy intermediate-scale quantum (NISQ) devices, variational algorithms such as VQE and QAOA combine quantum and classical computing [12]
Step-by-Step Process:

- A Hamiltonian for the system is defined.
- Prepare a parameterized quantum state.
- Measure the expectation value of the energy.
- Apply classical optimization (e.g., gradient descent) to parameters.
- Repeat until convergence.

E. Quantum Machine Learning

It investigates quantum algorithms such as quantum support vector machines to speed up machine learning calculations [18].

Step-by-Step Process:

- Represent classical data as quantum states.
- Implement quantum kernels to calculate similarities.
- Read out answers to train a model.

VI. Challenges and Future Directions

Quantum computing does have the potential to completely transform the character of solving more complex computational problems but there are a number of practical challenges which still require to be overcome before its use can become widely accepted. At this point, real-world applications are limited by factors such as low scalability, high error rates, extremely high hardware costs and inability to control the system with accuracy. The existing quantum computers have a small number of qubits, which is not scalable to the large-scale algorithms such as Shor. In addition, the noisy intermediate-scale quantum (NISQ) devices are also defined by the high frequency of operational errors caused by the distractions of the environment and an imprecise implementation of the gates, therefore, efficient error correction
is one of the highest priorities. Despite all these challenges, the development of topological qubits is encouraging, as
they are being developed to ensure that the system reduces decoherence and increases the stability of the system. Besides this, the services based on quantum technology as AWS Braket and Azure Quantum are now available, so access to quantum technology becomes more accessible due to remote access to quantum resources in familiar programming languages. These developments are facilitating more engagement, interdisciplinary collaboration, and innovation and signify the future that promises a shift of the trajectory in the study of quantum computing.

VII. Conclusion

The field of quantum computing is at the fringes of computer knowledge. It does not merely bring a couple of new tricks, it turns the entire concept of computing inside out. I presented the nuts and bolts in this paper, i.e. qubits, superposition, entanglement, quantum gates, measurement and coherence. I also touched some of the game-changing algorithms that have made us re-evaluate the capabilities of computers. The reality is evident- quantum computing brings in concepts and approaches that uproot all we believed about classical computing. It challenges us to rethink the way we approach security, algorithms and even the way we approach the construction of computer systems in the first place. The fundamental concepts of quantum computing are its key strength. Superposition is a technique that allows qubits [3] to operate on tons of possibilities simultaneously. The entanglement and quantum gates allow us to coordinate and reverse the operations which are simply impossible with ordinary computers. Measurement issues, probabilism, and decoherence actually point out how challenging this area becomes- and how effective it can be, with the additional assistance of things like surface codes [5] to work with. It is these notions that support algorithms such as Shors that essentially break RSA encryption due to its insane speed (Shor, 1994). The algorithm developed by Grover is also of the magic kind, thus the searches are faster (Grover, 1996). Quantum Fourier Transform increases the detectivity of periodicity, and hybrid methods extend the performance of the existing NISQ machines with variational algorithms such as VQE. And we should not overlook what is on the horizon, quantum machine learning will only accelerate the trend [12]. To begin with, quantum computers are posing a threat to the existing cryptography, and thus scientists are scrambling to install new post-quantum standards (NIST, 2022). And it is giving renewed fruit to algorithm design, such as the crazy quantum- inspired tensor networks [11]. Complexity theory? That's shifting, too. Quantum machines are capable of solving some problems in the BQP-class in a significantly more efficient manner than we had previously been able to do. However, this is not merely theory that you require hardware and software teams liaise and what it implies is that people of all types of backgrounds have to make contributions (see [2]). At the moment quantum computers do not exist in isolation. They are collaborating with classical systems in hybrid configurations and this is producing some rather exciting innovation, despite the fact that quantum technology is currently expensive and utilized in distinct applications. There are a few large obstacles, though. Scalability is sore since we have just a limited number of qubits to play with (IBM Eagle chip has 127 qubits to date). The devices we currently use are NISQ devices which are noisy and prone to errors. The expensive price locks many out. But that is not the only thing: it is challenging to control qubits precisely, the

software development process is complex, the systems do not all interact well, and quantum machines can consume huge amounts of power. This is all what is likely to make the technical and money challenges quite clear ([6]).

REFERENCES

[1] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J.C., Barends, R., Biswas, R., Boixo, S., Brandao, F.G., Buell, D.A., et al.: Quantum supremacy using a programmable superconducting processor. Nature 574(7779), 505–510 (2019)

[2] Gambetta, J.: IBM Quantum Roadmap. IBM Research. https://research.ibm. com/blog/quantum-roadmap-2023 Accessed 2023-01-01

[3] Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge university press, ??? (2010)

[4] Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134 (1994).

[5] Fowler, A.G., Mariantoni, M., Martinis, J.M., Cleland, A.N.: Surface codes: Towards practical large-scale quantum computation. Physical Review A—Atomic, Molecular, and Optical Physics 86(3), 032324 (2012)

[6] Preskill, J.: Quantum computing in the nisq era and beyond. Quantum 2, 79 (2018)

[7] Bernstein, D.J.: Post-quantum cryptography. In: Encyclopedia of Cryptography, Security and Privacy, pp. 1846– 1847.

[8] National Institute of Standards and Technology: Post-quantum cryptography standardization. Technical Report NIST IR 8413, U.S. Department of Commerce, National Institute of Standards and Technology (2022)

[9] Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. Theoretical computer science 560, 7–11 (2014)

[10] Bauer, B., Bravyi, S., Motta, M., Chan, G.K.-L.: Quantum algorithms for quantum chemistry and quantum materials science. Chemical reviews 120(22), 12685–12717 (2020)

[11] Or´us, R.: Tensor networks for quantum-inspired machine learning. Nature Reviews Physics 1(9), 538–550 (2019) https://doi.org/10.1038/ s42254-019-0086-7

[12] McClean, J.R., Romero, J., Babbush, R., Aspuru-Guzik, A.: The theory of variational hybrid quantum-classical algorithms. New Journal of Physics 18(2), 023023 (2016)

[13] Microsoft Quantum Team: Advances in Topological Quantum Computing. Microsoft. Microsoft Quantum Blog. https://cloudblogs.microsoft.com/ quantum/ Accessed 2024-01-01

[14] Dyakonov, M.: When will useful quantum computers be constructed? not in the foreseeable future, this physicist argues. here's why: The case against: Quantum computing. Ieee Spectrum 56(3), 24–29 (2019)

[15] Jaswal, K., Choudhury, T., Chhokar, R.L., Singh, S.R.: Securing the Internet of Things: A proposed framework. In: Proceedings of the IEEE International Conference on Computing, Communication and Automation (ICCCA 2017), pp. (2017). https://doi.org/10.1109/CCAA.2017.8230015

[16] Chaudhary, D.K., Lal, R., Kashyap, N., Choudhury, T.: Hybrid edge detection tech-nique for digital images. In: Proceedings of the IEEE International Conference on Com-puting, Communication and Automation (ICCCA 2016), pp. (2016). https://doi.org/10.1109/CCAA.2016.7813883

[17] Kashyap, N., Choudhury, T., Chaudhary, D.K., Lal, R.: Mood based classification of music by analyzing lyrical data using text mining. In: Proceedings of the International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE 2016), pp. (2016). https://doi.org/10.1109/ICMETE.2016.65

[18] Negi, P.S., Pawar, R., Lal, R.: Vision-Based Real-Time Human–Computer Interaction on Hand Gesture Recognition. In: Lecture Notes in Networks and Systems, pp. (2020). https://doi.org/10.1007/978-981-15-2329-851

[19] Garg, A., Bajaj, A., Lal, R.: Brain Tumor Detection Using Image Processing Based on Anisotropic Filtration Techniques. In: Lecture Notes in Networks and Systems, pp. (2020). https://doi.org/10.1007/978-981-15-2329-837

[20] Gupta, A., Choudhury, T., Lal, R.: An efficient scheme to secure cloud with diversified fortified mechanisms. In: Proceedings of the International Conference on Big Data Ana-lytics and Computational Intelligence (ICBDACI 2017), pp. (2017). https://doi.org/10.1109/ICBDACI.2017.8070829

[21] Lal, R., Singh, S.P., Garg, A., Negi, P.S.: Brain tumor detection using PSO–FCM based segmentation. International Journal of Engineering and Advanced Technology 9(1), (2019). https://doi.org/10.35940/ijeat.A1903.109119.