iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.70361

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Quantum Computer: *A Revolutionary Technology*

Niraj Patil[1], Sadhana Jadhav[2], Prof. R. Pande[3]
[1, 2]*Electronics and Computer, Engineering Kolhapur, India*
[3]*Project Guide*

Abstract: ***For certain complex problems, quantum computers offer a significant speed advantage over classical computers by leveraging principles such as superposition and entanglement. This paper explores the potential of quantum computing in fields like cryptography, drug discovery, artificial intelligence, and optimization, while also addressing existing research challenges and limitations.***
Keywords: Quantum computing, qubits, superposition, quantum algorithms, applications, challenges.

I. QUANTUM COMPUTING

With fresh ideas that go beyond the constraints of classical computing, quantum computing represents a fundamental shift in computational science. Quantum computers use quantum bits (qubits), which can exist in multiple states simultaneously due to superposition, as opposed to traditional computers, which process information using binary bits (0s and 1s). Quantum systems also take advantage of entanglement, which makes it possible for qubits to be inherently connected and facilitates much more effective calculations. These quantum mechanical ideas could be used by quantum computing to solve difficult issues that are beyond the capabilities of traditional systems, with significant implications for domains like material science, artificial intelligence, and cryptography.

II. WHAT IS A QUANTUM COMPUTER?

A quantum computer is a modern computational device that outperforms classical computers by processing information in a completely new way using the concepts of quantum mechanics. Quantum computers use qubits, which can exist as 0, 1, or both simultaneously due to superposition, compared to traditional computers that use bits, which exist as either 0 or 1. Because of this special characteristic, quantum systems can execute several calculations simultaneously, significantly increasing their computational capacity.

Quantum computers use parallelism to solve complex problems much more quickly than classical machines, which process data sequentially.

Quantum computers take advantage of entanglement, a phenomenon in which qubits become inherently linked—that is, the state of one qubit directly influences the state of another, Because of their interconnection, quantum computers are able to process enormous volumes of data and perform extremely efficient computations in ways that are not possible with classical computers. These characteristics make quantum systems superior in domains like material science, artificial intelligence, cryptography, and optimization that demand enormous amounts of processing power. Quantum computers can investigate several solutions at once, which makes them especially helpful for problems with many potential solutions, in comparison with classical systems that depend on methodical computations.

III. ANALOGY

Imagine navigating a vast video game world where progress is contingent upon solving complex equations to get an understanding of the distinction.

We first solved these equations by hand, which was slow and constrained, like walking. Traditional computers functioned similarly to automobiles, increasing the effectiveness of problem-solving. However, quantum computers are more than just faster automobiles; they offer a completely new mode of transportation, similar to boats navigating an ocean, which makes it possible to reach previously inaccessible places.

Quantum computers provide revolutionary breakthroughs in scientific research, encryption, and practical problem-solving by redefining computation through the principles of quantum mechanics. Even though they are still in their early years, further advancements in quantum hardware, error correction, and algorithm development will influence computing in the future and open up possibilities beyond traditional limitations.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

IV. CLASSICAL VS QUANTUM COMPUTING

Transistors that alternate between 0 and 1 are used in classical computers to process information in sequential order. These systems take a methodical approach, using a sequence of logical operations to solve issues. Even though classical computing is very good at many things, it is not very good at solving problems that need a lot of processing power, like deciphering encryption algorithms or predicting molecular structures.

Quantum computers, on the other hand, use qubits, which use quantum phenomena like entanglement and superposition to carry out computations in an uncommon manner. Quantum computers may explore multiple solutions at once because superposition enables qubits to exist in multiple states simultaneously. By connecting qubits, entanglement further improves computational efficiency and enables complex problem-solving that is beyond the scope of classical methods.

V. FUNDAMENTALS OF QUANTUM COMPUTING

A. QuBits

Unlike classical bits, which only exist as 0 or 1, qubits, also known as quantum bits, are the basic building block of quantum computing. However, qubits use the principles of quantum mechanics to exist in multiple states at the same time. Because of this special property, quantum computers can execute calculations in parallel, significantly increasing computational speed and efficiency. Qubits enable accelerating scaling in processing power, in contrast to classical computers that process data sequentially. Extreme precision is necessary to maintain a qubit's quantum state, though, because environmental interactions can lead to decoherence, which can interfere with computations. Researchers create sophisticated quantum architectures and error correction methods to overcome these obstacles. despite these challenges, qubits have the potential to solve a wide range of challenging issues that traditional computers find difficult to handle, including large-scale optimizations, molecular modeling, and cryptography.

B. Superposition

Unlike classical bits, which are restricted to a single binary state, qubits can exist in multiple states simultaneously thanks to a fundamental principle in quantum mechanics called superposition. This enables quantum computers to investigate numerous potential solutions in parallel since a single qubit can represent both 0 and 1 at the same time. For instance, a quantum computer can analyze all possible outcomes at once, significantly cutting down on computation time for complex problems, whereas a classical computer must evaluate various possibilities sequentially. This benefit has drawbacks, though, as the qubit loses its superposition and collapses into a single state (either 0 or 1) upon performing a measurement. Superposition is used by sophisticated quantum algorithms, like Grover's search algorithm and Shor's factorization algorithm, to achieve revolutionary computational efficiency that goes beyond classical bounds.

1) Shor's Algorithm (Factorization)

In 1994, mathematician Peter Shor created Shor's algorithm, a quantum algorithm that effectively divides large numbers into their prime components. The foundation of contemporary encryption systems like RSA encryption is the computational difficulty of factoring very large numbers in classical computing. When factoring numbers with hundreds of digits, a traditional computer would take an unreasonably long time because it would have to check a large number of potential factors one after the other. However, Shor's algorithm is used by quantum computers to solve this problem exponentially more quickly. The algorithm effectively determines the prime factors of a given number by using periodicity and quantum Fourier transforms. This discovery puts traditional cryptography techniques in risk because it makes it possible to crack RSA encryption, which was previously thought to be impossible in a reasonable amount of time, with powerful enough quantum hardware.

2) Grover's Algorithm (Search)

Grover created the quantum search algorithm known as Grover's algorithm in 1996 with the goal of greatly accelerating database searches. In traditional computing, it takes an average of N/N/2 items to search through an unsorted database of N N elements before locating the right one. In the worst case, checking all N items is necessary, which takes a lot of time for large datasets.

Grover's algorithm reduces search time from (N) O(N) to $O(N)$ O(N) by providing a quadratic speedup. It does this by mathematically enhancing the correct solution through amplitude amplification and quantum superposition. Grover's algorithm has significant uses in data mining, artificial intelligence, and cryptography, especially in breaking symmetric encryption by cutting down on brute-force search time, even though its speedup is not as dramatic as Shor's algorithm.

©IJRASET: All Rights are Reserved

C. Entanglement

A quantum phenomenon known as entanglement occurs when two or more qubits become inextricably linked, meaning that regardless of their distance from one another, the state of one qubit instantly affects the state of another. This makes it possible for quantum computers to operate more efficiently than traditional computers.

Entangled qubits share information instantly, in contrary to classical systems that transmit information step-by-step. This characteristic is essential for distributed quantum computing, secure communication, and quantum teleportation. Entanglement is fragile, though, because outside interference can result in decoherence and sever the quantum connection. To maintain entanglement over time, researchers are attempting to create fault-tolerant quantum systems and enhance quantum error correction. To fully utilize quantum computing in complex simulations, optimization, and cryptography, entanglement must be used effectively.

VI. HOW QUANTUM COMPUTERS WORK

Manipulate qubits, quantum computers function fundamentally differently from classical computers. By utilizing the concepts of superposition and entanglement, these gates allow quantum systems to execute intricate computations at an exponentially faster rate than their classical counterparts. Quantum gates work with superposed qubits, enabling them to process multiple states at once, in contrast to classical logic gates (AND, OR, NOT), which process bits systematically (one state at a time). This makes it possible for quantum computers to perform calculations in parallel, which significantly cuts down on processing time for some tasks.

1) Hadamard Gate (H): Creates superposition by transforming a qubit from a definite state (0 or 1) into a 50-50 probability of being either. This is crucial for parallel computing.
2) Pauli Gates (X, Y, Z): Analogous to classical NOT gates but applied in a quantum way, flipping or rotating qubit states.
3) CNOT Gate (Controlled-NOT): Implements entanglement by flipping a target qubit based on the state of a control qubit, forming the foundation for quantum parallelism.
4) Toffoli Gate: A universal quantum gate used in error correction and reversible computation.
5) Phase Gates (S, T): Modify the phase of a qubit's quantum state, essential for complex quantum algorithms.

VII. QUANTUM MEASUREMENT AND DECOHERENCE

Measurement is one of the main problems with quantum computing. When a qubit is measured, its quantum advantage is lost and its quantum state is collapsed into either 0 or 1, in contrast to classical bits that can be read directly. Quantum algorithms reduce direct measurements until the very end of the computation process in order to counteract this. Decoherence, in which noise from the environment disturbs quantum states and results in information loss, is another significant problem. Researchers counter this by preserving quantum information and enhancing computation reliability through the use of quantum error correction (QEC) techniques like Shor's Code and surface codes.

VIII. PRINCIPLES IN QUANTUM COMPUTING

A. Probability Amplitudes and Wave Function

A system's quantum state is described by a wave function (Ψ) in quantum mechanics. It shows the probability intensity of the energy, momentum, or position of a particle. The wave function collapses to a specific state upon measurement (0 or 1 in a qubit). Qubits can be both 0 and 1 simultaneously until they are measured because their wave function exists in a superposition of states. Because of this characteristic, quantum computers can investigate several computational avenues at once as opposed to one at a time.

B. Quantum Tunneling

When a particle traverses a potential barrier that would be impossible to cross in classical physics, this phenomenon is known as quantum tunneling. D-Wave Systems uses a computing technique called quantum annealing, which takes advantage of this phenomenon to solve optimization problems by letting quantum states tunnel toward the optimal solution, or lowest energy configuration.

C. Interference of Quantum

In order to help quantum algorithms amplify right answers and suppress wrong ones, quantum interference occurs when probability waves reinforce or cancel each other out. Interference is used by Grover's algorithm for search and Shor's algorithm for factorization to produce quadratic and exponential speedups, respectively.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

D. Zero-Point Energy and Quantum Fluctuations

The Heisenberg Uncertainty Principle, which states that energy levels in a vacuum fluctuate continuously, causes quantum fluctuations. These fluctuations have an impact on certain quantum computing architectures, such as superconducting qubits, leading to specific designs to ensure stability.

IX. HOW THESE PRINCIPLES IMPACT QUANTUM COMPUTING

Problems that are significantly harder for classical systems can be solved by quantum computers through the use of interference, wave function manipulation, and quantum tunneling. The realization of large-scale quantum computing will depend on future developments in coherence time, quantum error correction, and new qubit designs.

A. Advantages of Quantum Computing

1) Exponential Speedup – Solves complex problems much faster than classical computers.
2) Parallel Processing – Uses superposition to perform multiple calculations simultaneously.
3) Optimized Problem-Solving – Quickly finds solutions for logistics, finance, and AI.
4) Revolutionizing Artificial Intelligence – Enhances machine learning and pattern recognition.
5) Breakthroughs in Cryptography – Enables secure quantum encryption (QKD).
6) Advanced Scientific Simulations – Accurately models molecular structures and quantum systems.
7) Superior Financial Modeling – Improves risk analysis, fraud detection, and trading strategies.
8) Faster Drug Discovery – Simulates chemical reactions to develop new medicines.
9) Improved Climate Modeling – Enhances weather predictions and climate simulations.
10) Energy Efficiency & Sustainability – Optimizes power grids and renewable energy sources.
11) High-Performance Data Processing – Handles big data more efficiently.
12) Quantum-Secure Communications – Protects data from cyber threats.

B. Disadvantages of Quantum Computing

1) Hardware Complexity – Requires highly controlled environments (near absolute zero) to maintain qubit stability.
2) Qubit Instability (Decoherence) – Quantum states are fragile and easily disrupted by external noise.
3) Error Rates & Noise – Current quantum computers have high error rates due to imperfect qubit control.
4) Limited Qubit Scalability – Scaling up qubits while maintaining stability is a major challenge.
5) Short Coherence Time – Qubits lose their quantum state quickly, limiting computation time.
6) Extremely Expensive – Developing and maintaining quantum systems costs millions of dollars.
7) Lack of Standardization – No universal quantum computing architecture exists yet.
8) Algorithm Development – Few practical quantum algorithms are available for real-world applications.
9) Threat to Classical Cryptography – Quantum computers could break RSA and ECC encryption.
10) Limited Commercial Applications – Still in experimental stages with few practical use cases.
11) High Energy Consumption for Cooling – Requires cryogenic cooling to operate properly.
12) Specialized Knowledge Required – Quantum computing requires expertise in physics, mathematics, and quantum mechanics.

C. Areas to Explore with Quantum Computing

1) Drug discovery and medicine: By simulating molecular interactions at the atomic level, quantum computers can greatly speed up the creation of new drugs, vaccines, and individualized therapies. They can also aid in the development of focused treatments for complicated illnesses like Alzheimer's and cancer.
2) Materials Science: By using quantum simulations, scientists can find new materials with ideal characteristics, like ultra-strong alloys, high-temperature superconductors, and sophisticated battery materials for energy storage.
3) Artificial Intelligence & Machine Learning: By accelerating the training of AI models and advancing fields like natural language processing, autonomous systems, and recommendation algorithms, quantum computing can improve deep learning, pattern recognition, and optimization.
4) Climate Science & Weather Prediction: By enhancing climate models, quantum simulations enable researchers to more precisely examine carbon capture methods, extreme weather trends, and environmental preservation tactics.

©IJRASET: All Rights are Reserved

5) Cybersecurity and Cryptography: Although quantum computers threaten well- established encryption techniques like RSA, they also make quantum cryptography possible, like quantum key distribution, or QKD, which guarantees impenetrable security for private information.
6) Financial Modeling & Risk Analysis: By optimizing stock market forecasts, fraud detection, portfolio management, and financial risk assessments, quantum algorithms help businesses make more informed decisions.
7) Supply Chain & Logistics: Businesses can improve transportation, delivery, and resource allocation efficiency by using quantum optimization algorithms to solve intricate routing and logistics issues.
8) Aerospace & Defense: By enhancing satellite communications, defense encryption, autonomous navigation, and spacecraft materials, quantum computing can improve space exploration and national security.

REFERENCES FOR QUANTUM COMPUTING RESEARCH

Wikipedia
[1] General knowledge on quantum computing principles, algorithms, and applications. (https://en.wikipedia.org/wiki/Qua ntum_computing)

Research Papers & Journals
[1] Nielsen, M.A., & Chuang, I.L. (2010). Quantum Computation and Quantum Information. Cambridge University Press.
[2] Arute, F. et al. (2019). Quantum Supremacy Using a Programmable Superconducting Processor. Nature, 574(7779), 505-510. (Google AI Quantum Research)
[3] Preskill, J. (2018). Quantum Computing in the NISQ Era and Beyond. Quantum, 2, 79. (arXiv:1801.00862)

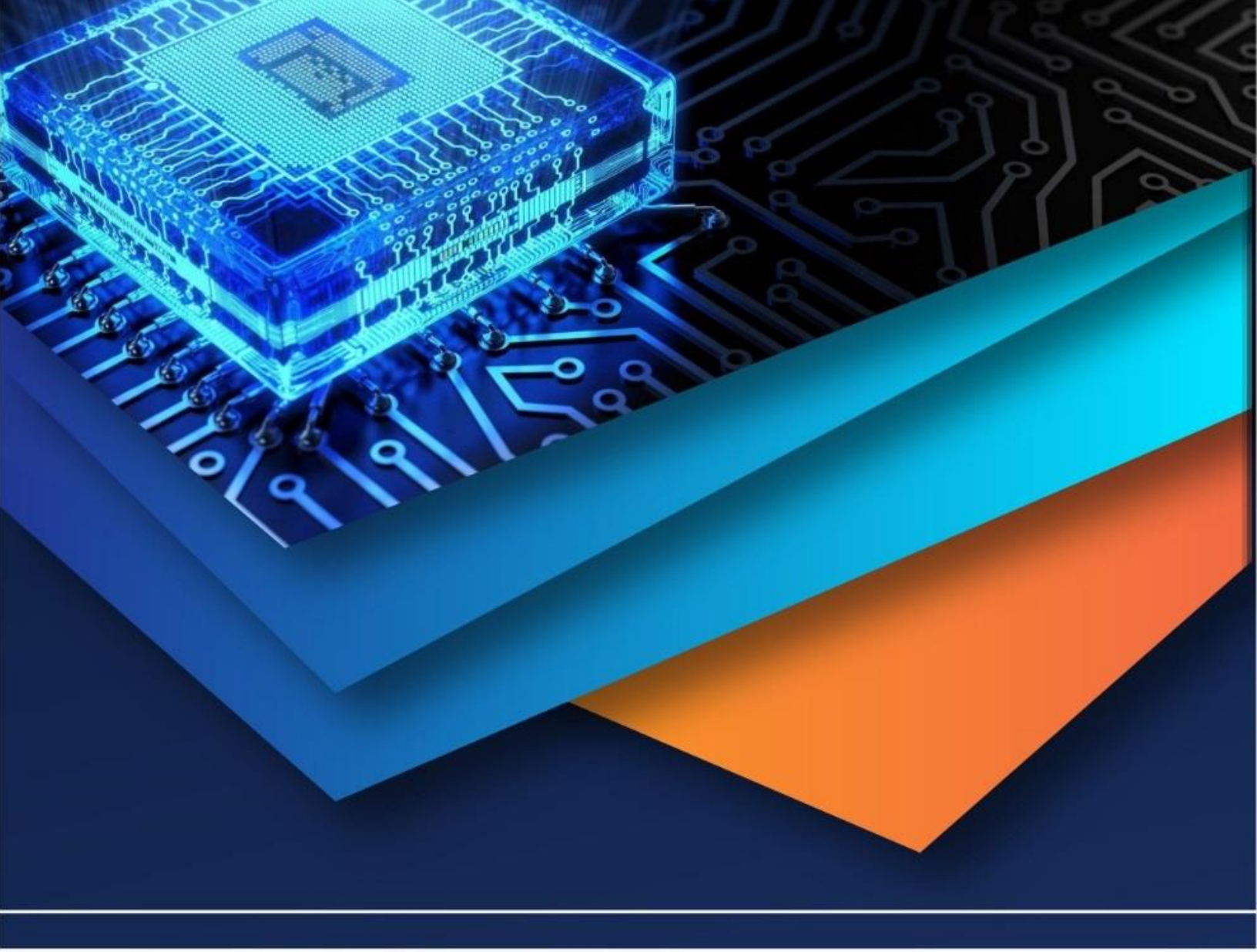
YouTube Videos & Lectures
[1] Veritasium – How Quantum Computers Break Encryption
[2] MIT OpenCourseWare – Introduction to Quantum Computing
[3] PBS Space Time – Quantum Computing & The Many Worlds Interpretation
[4] IBM Quantum – How Qubits Work

Books
[1] Aaronson, S. (2013). Quantum Computing Since Democritus. Cambridge University Press.
[2] Das Sarma, S. (2023). Quantum Computing: What It Is and What It Will Be. Harvard University Press.
[3] Kaye, P., Laflamme, R., & Mosca, M. (2007). An Introduction to Quantum Computing. Oxford University Press.

Official Research & Company Reports
[1] Google Quantum AI (https://quantumai.google/)
[2] IBM Quantum Computing Research (https://www.ibm.com/quan tum)
[3] Microsoft Quantum Computing (https://www.microsoft.com/en-us/quantum/)

Chat GPT
[1] Assisted in refining and expanding research content with professional, detailed explanations.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)