

Quantum Computing :Circuits, Algorithms and Application

Mr. Pradeep Nayak¹, Sudeep Rathod², Surabhi³, Sukanya⁴

Department of Information Science and Engineering¹⁻⁴

Alva's Institute of Engineering and Technology, Mijar, Karnataka, India

Abstract: *With its potential to completely change computation, quantum computing—a groundbreaking discipline that sprung from computer science and quantum mechanics—has attracted a lot of interest. This essay attempts to cover the foundations of quantum computing and offer a thorough manual for readers who are not specialists in the subject. We start by going over the basic ideas of quantum computing and then take readers through the concepts of qubits, superposition, entanglement, interference, and noise. We study quantum gates, quantum hardware, and fundamental quantum circuits. This paper provides an overview of the present state of quantum computing, focusing on the noisy intermediate-scale quantum (NISQ) era and its possible applications to practical issues. delve into the creation of quantum algorithms and their uses, emphasizing well-known algorithms like as Grover's and Shor's. We also discuss how several fields, like material science, machine learning, encryption, and optimization, are affected by quantum computing. Upon finishing this paper, readers will possess a firm grasp of the fundamentals, practical uses, and procedures of quantum circuit development. Our objective is to offer an invaluable resource for scholars hoping to keep current on this quickly developing topic as well as for those ready to start their adventure with quantum computing.*

Keywords: Quantum Computing, Qubits, Quantum circuits, Noise Measurement

I. INTRODUCTION

When solving certain computational problems, quantum computing technology uses novel techniques that result in higher efficiency when compared to classical computing systems. The promising results of recent experiments imply that quantum computing could be commercially available very soon. When it comes to solving specific computational problems, quantum computing technology is far more efficient than classical computing systems because it uses different techniques. The promising results of recent experiments suggest that quantum computing could be available commercially very soon. Certain parts, such registers, gates, and memory components, are shared by quantum and conventional computers. They have essentially different and separate physical structures, nevertheless [1]. Where qubits may reside in both the superposed and entangled states, quantum calculations take place within quantum registers. Quantum computers are essentially distinct from conventional classical computers due to these special qualities. Quantum mechanics, a foundational theory of physics that describes nature at the tiniest sizes of energy levels of atoms and subatomic particles, provides the basis for quantum computing, a sophisticated branch of computing [2]. When it comes to information, quantum computers employ quantum bits, or qubits, as opposed to classical computers that use bits.

HISTORY

Unlike classical computing, quantum computing is a relatively new technology. Its inception dates back to sciencefiction in the late1970s, when it first surfaced and garnered media attention. Richard Feynman is recognized as having

invented the idea of a quantum computer in 1981. He put out the theory that quantum computers might effectively model quantum processes, avoiding the exponential resource needs of conventional computers [3]. Quantum system simulation poses significant challenges for classical computers. Feynman realized the enormous potential of quantum computers in the domain of challenging computing problems, as did pioneers like Yuri Manin and Paul Benioff. By

using quantum bits rather than conventional bits, classical and quantum computers vary significantly from one another [4]. This class of "qubits" is the classical bit's quantum mechanical counterpart [5]. As long as a qubit is not being measured, it exists in a state known as superposition. Accordingly, it exists in both of the two states concurrently and only when measured does it break down into one of the two states with a certain probability. A photon with its polarization measured in two orthogonal directions might be thought of as a potential physical realization of a qubit.

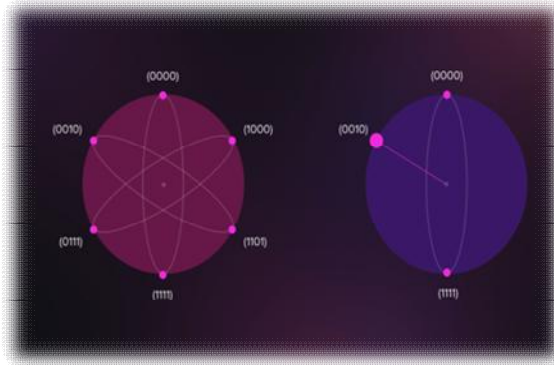


Fig: Quantum Computing

II. QUANTUM COMPUTING FUNDAMENTALS

Quantum computing uses qubits, which may exist in several states simultaneously—a phenomenon known as superposition—in place of bits, which are used in traditional computing. Quantum entanglement denotes a special relationship between qubits, and quantum interference modifies the qubit's behaviour. Another difficulty facing quantum computers is quantum noise, which can alter the behaviour of a quantum system and result in the loss of quantum features including superposition, entanglement, and interference [6]. The goal of this part is to give a basic, yet thorough, grasp of the principles of quantum computing.

Qubit: The fundamental building block of quantum information in quantum computing is known as a qubit, or quantum bit. A qubit, in contrast to a classical bit, can exist concurrently in a superposition of both states, instead of only being 0 or 1. This characteristic allows quantum computers to do some computations far more quickly than classical computers, combined with entanglement and quantum interference.

Standard representation of Qubit: Two orthonormal basis states, also known as basis vectors, can be linearly superposed to describe a qubit's general quantum state in quantum mechanics. These vectors are usually denoted as $|0\rangle = (10)$ and $|1\rangle = (01)$. They are written in conventional Dirac – or – “bra -ket” notation. $|0\rangle$ and $|1\rangle$ are pronounced, respectively, as “ket 0” and “ket 1”. Both of these orthonormal basis states, $\{|0\rangle, |1\rangle\}$ Together, these values, referred to as the computational basis, cover the two-dimensional linear vector (Hilbert) space of the qubit. Qubit basis states can also be combined to form product basis states. A set of qubits taken together is called a quantum register [7]. A quantum register is a collection of qubits used to store quantum information. In quantum computing, quantum registers serve a similar role to classical registers in classical computing, but they harness the principles of quantum mechanics to enable complex computations.

Qubit States: In quantum computing, qubit states—which stand for quantum bits—are the basic building blocks of information. Qubits are different from traditional bits in that they may exist in a simultaneous superposition of both states (0 and 1). A thorough description of qubit states may be found here

Basis States: The most basic states of a qubit are the computational basis states: $|0\rangle = (10)$ and $|1\rangle = (01)$

Superposition: A qubit can be in a superposition of the basis states $|0\rangle$ and $|1\rangle$. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where $|\alpha|^2 + |\beta|^2 = 1$. These coefficients represent the probability amplitudes of the qubit being in each state. The probabilities of measuring the qubit in states $|0\rangle$ respectively.

Bloch Sphere: Qubit states can be visualized using the Bloch sphere, a unit sphere where any pure qubit state corresponds to a point on the surface of the sphere. The state $|\psi\rangle$ can be represented as $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi} \sin(\theta/2)|1\rangle$.

The absolute value (magnitude) of this term is always 1 regardless of the value φ .
(i.e, the magnitude of α and β is determined by θ only)

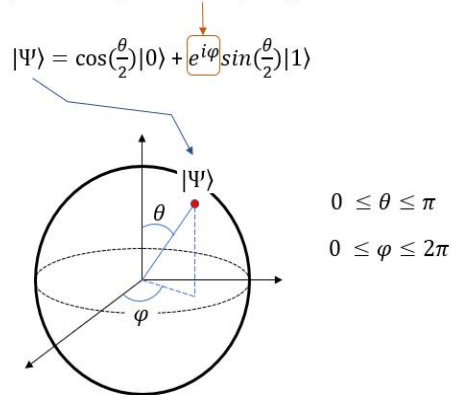


Fig. Block Sphere

The surface of the Bloch sphere is a twodimensional space, which represents the observable state space of the pure qubit states. This state space has two local degrees of freedom, which can be represented by the two angles θ and ϕ .

III. QUANTUM CIRCUITS

The two fundamental components of quantum circuits are measurement and quantum gates. Similar to conventional logic gates, quantum gates are crucial components of quantum circuits. By manipulating qubits, these gates enable the conversion of quantum information. The several kinds of quantum gates—Hadamard, CNOT, and Pauli gates, among others—that are the building blocks of quantum circuits are explained in this section. This section also covers the crucial phase of quantum measurement, which is the collapse of qubit superposition into distinct states. Time is inscribed on a circuit in such a way that it runs from left to right along the horizontal axis [8]. Classical bits are represented by doubled lines, and qubits by horizontal ones. Measurements or gates are examples of the qubit-operated objects that are connected via these lines. Usually not actual wires, these lines specify the order in which things happen.

Components of Quantum Circuits:

Qubits: The basic units of quantum information. Each qubit can exist in a superposition of states $|0\rangle$ and $|1\rangle$.

Quantum Gates: Operations that change the state of qubits. These gates are the quantum analogs of classical logic gates (like AND, OR, NOT) but can also create superpositions and entanglements

Quantum Wires: Represent the passage of qubits through time and gates in a quantum circuit diagram.

Measurement: The process of collapsing qubits to classical bits $|0\rangle$. Measurements are typically performed at the end of a quantum circuit. This is an entangled state, known as a Bell state.

The basis for quantum computation is provided by quantum circuits, which allow complicated algorithms that are computationally impractical for conventional computers to be executed with ease through the manipulation and measurement of qubits. Quantum circuits hold the potential to transform domains like cryptography, materials science, and optimization by utilizing distinct quantum phenomena like superposition and entanglement. Building and comprehending quantum circuits will be essential to utilizing quantum technologies to their maximum potential as quantum computing research and development advance.











Operator	Gate(s)	Matrix
Pauli-X (X)	 \oplus	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

Fig. Quantum Circuits

IV. NOISE MEASUREMENT

The uncertainty and fluctuations that occur in quantum systems as a result of quantum mechanics' probabilistic character are referred to as quantum noise. Even at low temperatures, quantum systems present difficulties. Noise in classical systems is frequently related to random fluctuations in signals or outside disturbances. A quantum system in a superposition state has a measurement output that depends on the probability distribution of the quantum states rather than a deterministic one [9]. The quantum system's contact with the outside world can introduce noise and mistake into the result. Over time, it may result in the loss of quantum features, such as superposition, entanglement, and interference, which might have an impact on how quantum circuits perform.

Noise distributions refer to the statistical patterns that describe the nature of the noise present in data. Various types of noise distributions are commonly encountered in different fields such as signal processing, statistics, and machine learning [10].

Here are some common types:

1. Gaussian (Normal) Noise:

- Description: Gaussian noise is the most common type of noise distribution, characterized by its bell-shaped curve (normal distribution). It is defined by its mean (average value) and variance (spread).
- Applications: Often assumed in statistical models and is prevalent in many natural and man-made processes.

2. Uniform Noise:

- Description: In a uniform noise distribution, every value within a certain range is equally likely. This distribution is flat, unlike the peaked Gaussian distribution.
- Applications: Often used in simulations and scenarios where all outcomes are equally likely.

3. Poisson Noise:

- Description: Poisson noise is a type of noise where events occur independently with a known average rate. It is often used to model count-based data.

- Applications: Common in photon counting, network traffic, and other processes where events occur randomly in time or space.
- 4. Salt-and-Pepper Noise:**
- Description: This is a type of noise where the data is corrupted by random occurrences of black and white pixels (for images) or minimum and maximum values (for other data types).
 - Applications: Common in image processing where it models random occurrences of extreme pixel values.
 - Characteristics: Appears as sparsely occurring white and black pixels.
- 5. Exponential Noise:**
- Description: Exponential noise is often used to model the time between events in a Poisson process. It is a skewed distribution with a longer tail on one side.
 - Applications: Often found in reliability analysis and queuing theory.
- 6. Laplacian (Double Exponential) Noise:**
- Description: Laplacian noise has a sharper peak at the mean and heavier tails compared to Gaussian noise. It is useful when modelling data with outliers.
 - Applications: Often used in applications requiring robust statistics.
- 7. Gamma Noise:**
- Description: Gamma noise is used in processes where the noise is not symmetric and is skewed towards one direction.
 - Applications: Often used in signal processing and finance.
- 8. Rayleigh Noise:**
- Description: Rayleigh noise distribution is used when the magnitude of a vector whose components are independent and identically distributed Gaussian is considered.
 - Applications: Often seen in signal processing and radar systems.
- 9. Speckle Noise:**
- Description: Speckle noise is a granular noise that inherently exists in and degrades the quality of images and synthetic aperture radar data.
 - Applications: Common in radar and medical imaging.
 - Characteristics: Results from the random interference of multiple waveforms.

Understanding these different noise distributions is important for properly modelling and mitigating noise in data, which is critical in fields like machine learning, image processing, and statistics.

Mathematically, the classical additive white Gaussian noise and the quantum Poisson noise are simultaneously characterized as $Z=Z_1+Z_2$, where Z_1 is the Poissonian-distributed noise resulting from quantum fluctuations and Z_2 is the Gaussian-distributed classical equivalent. By treating Z as the convolution product of Z_1 and Z_2 , the statistical description of the hybrid classical-quantum noise Z is computed.

V. ALGORITHMS

Quantum algorithms have special abilities and uses that make them better than traditional algorithms in certain tasks. For example, Shor's algorithm can factor large numbers much faster than classical methods, and Grover's algorithm can search through databases more efficiently [11]. These and other quantum algorithms could significantly change how we approach computing.

1. Deutsch-Jozsa Algorithm

The Deutsch-Jozsa algorithm is a quantum algorithm that can solve the Deutsch-Jozsa problem. This has to do with figuring out if a certain Boolean function—one that yields the values "true" or "false"—is balanced or constant. One of the first quantum algorithms for this problem is the Deutsch-Jozsa algorithm, which is provably far quicker than is achievable in a classical setting. It is a more sophisticated version of the original Deutsch algorithm. Its foundation is the Fourier transform technique in its quantum iteration. Beginners can also benefit from the Deutsch-Jozsa algorithm's assistance in understanding the fundamentals of qubits and quantum computing. Consequently, it also aids in

illustrating the challenges associated with quantum computing. The IBM quantum computer has already been used for experimental implementations of this procedure, demonstrating its superior efficiency over traditional techniques.

2. Bernstein-Vazirani Algorithm

The Bernstein-Vazirani quantum algorithm takes advantage of quantum mechanics to infer information about a hidden string and determine it in fewer steps than classical algorithms, even when noise is present and the equipment is not operating at peak efficiency. Consequently, with or without noise, classical algorithms suffer from rapidly decreasing efficiency for large strings. The probability of correctly determining the string depends more on the overall level and fluctuation of noise and less on the type of noise. Therefore, the findings show that the Bernstein-Vazirani algorithm outperforms traditional methods in most situations. This cryptographic algorithm demonstrates the superiority of quantum computing for specific problems and is likely to be employed in cryptography.

3. Simon's Algorithm

Simon's algorithm is a quantum algorithm used to efficiently determine the period of a vectorial Boolean function, offering an exponential speed-up over classical algorithms [12]. This algorithm has applications in quantum cryptanalysis and cryptography, particularly in identifying patterns in the autocorrelation and Walsh spectrum of Boolean functions. Simon's algorithm is instrumental in developing a lightweight encryption algorithm, SIMON-GCM, which combines the SIMON cipher block with Galois/Counter Mode (GCM) for Internet of Things security. Evaluations have been conducted to assess its effectiveness in cryptanalysis.

4. Shor's Algorithm

Shor's algorithm, developed by mathematician Peter Shor in 1994, for factorizing numbers into their prime factors. This algorithm poses a significant threat to popular encryption methods like RSA, which rely on the difficulty of large integer factorization for security. Shor's algorithm leverages quantum properties such as superposition and entanglement to factor numbers much faster than classical methods. Essentially, given a number (n) that is the product of two prime numbers (p) and (q) , Shor's algorithm efficiently finds these prime factors. Although the implementation becomes increasingly complex with larger numbers, Shor's algorithm has demonstrated that quantum computing could potentially break widely used encryption schemes. Consequently, new cryptographic techniques need to be developed to resist future quantum attacks.

5. Grover's Algorithm

Grover's algorithm is a quantum algorithm that does substantially faster searches than conventional techniques in an unsorted database or list for a given value. It provides a quadratic speedup, which means that instead of the (N) steps required by conventional algorithms, where (N) is the number of items in the database, it can discover the item in roughly (\sqrt{N}) steps. One important illustration of how quantum computing can outperform classical computers in solving specific search and optimization tasks is the Grover's algorithm. It demonstrates the substantial benefits of quantum computing for particular jobs, as suggested by Lov Grover in 1996. However, Grover's technique alone won't provide polynomial-time solutions for these more complicated issues because it only offers a quadratic speedup whereas conventional approaches for NP-complete problems require exponentially more steps.

VI. APPLICATIONS

1. Cryptography:

Quantum Key Distribution (QKD)

Principle: Quantum key distribution uses quantum mechanics to enable two parties to produce a shared random secret key, which can be used to encrypt and decrypt messages. The security comes from the fact that measuring quantum data disturbs it, making eavesdropping detectable.

Protocols: The BB84 protocol, proposed by Bennett and Brassard in 1984, is the first and most widely implemented QKD protocol. It involves transmitting qubits in different bases (e.g., using the polarization states of photons) and using classical communication to ensure security [12].

Breaking Classical Encryption

Shor's Algorithm: In 1994, Peter Shor developed an algorithm that can factorize large integers and compute discrete logarithms efficiently on a quantum computer. This poses a threat to classical cryptographic systems like RSA and ECC, which rely on the difficulty of these problems.

Impact: The potential of quantum computers to break these cryptographic systems necessitates the development of quantum-resistant algorithms, known as post-quantum cryptography.

2. Optimization Problems:

Combinatorial Optimization

QAOA: The Quantum Approximate Optimization Algorithm (QAOA) is designed to solve combinatorial optimization problems. It combines classical and quantum computing techniques to find approximate solutions to problems like the Max-Cut problem and other NP-hard problems.

Application Example: In finance, QAOA can optimize trading strategies by finding the best combinations of assets to maximize returns or minimize risk.

Supply Chain Management

Traveling Salesman Problem (TSP): TSP seeks the shortest possible route that visits a set of cities and returns to the origin city. Quantum computing can solve TSP more efficiently, saving time and resources.

Vehicle Routing Problem (VRP): Similar to TSP, VRP involves finding the optimal routes for multiple vehicles to deliver goods to various locations. Quantum algorithms can provide better solutions faster than classical methods.

3. Material Science:

Simulating Molecular Structures

Quantum Simulations: Quantum computers can simulate the electronic structure of molecules with high precision, helping chemists understand molecular properties and reactions. Classical computers struggle with these simulations due to the exponential increase in computational resources needed.

Drug Discovery: By simulating molecular interactions, quantum computing can accelerate the identification of drug candidates and reduce the need for costly laboratory experiments.

Catalyst Design

Industrial Catalysts: Quantum computing can aid in designing catalysts that enhance chemical reactions, which is crucial for various industries, including pharmaceuticals and petrochemicals. These catalysts can make processes more efficient and environmentally friendly.

Environmental Impact: Quantum simulations can help develop catalysts that reduce harmful emissions, contributing to cleaner industrial processes.

4. Machine Learning:

Quantum Machine Learning (QML)

Enhanced Data Processing: Quantum algorithms like the Quantum Support Vector Machine (QSVM) and Quantum Principal Component Analysis (QPCA) can improve the speed and accuracy of machine learning tasks, handling larger datasets more efficiently.

Variational Quantum Circuits: These circuits are used to optimize machine learning models by adjusting parameters to minimize error, potentially offering better performance than classical methods.

5. Pharmaceuticals and Drug Discovery:

Drug Design and Discovery

Simulation of Drug Interactions: Quantum simulations can accurately predict how a drug interacts with its target, reducing the trial-and-error phase in drug development and speeding up the process of bringing new drugs to market.

Efficiency: By understanding molecular interactions at a quantum level, researchers can design more effective and specific drugs.

Protein Folding

Understanding Diseases: Accurate simulations of protein folding can lead to better understanding of diseases like Alzheimer's and Parkinson's, which are associated with misfolded proteins.

Drug Development: Facilitates the design of drugs that can effectively interact with specific protein structures, potentially leading to cures for currently untreatable diseases.

6. Financial Services

Risk Analysis and Portfolio Optimization

Optimization Algorithms: Quantum algorithms can solve large-scale optimization problems, such as portfolio optimization, more efficiently than classical algorithms, offering better risk management and asset allocation.

Monte Carlo Simulations: Quantum computers can speed up Monte Carlo simulations, which are used extensively in financial modeling and risk assessment.

Pricing Derivatives

Complex Financial Instruments: Derivatives pricing involves complex mathematical models that can be computationally intensive. Quantum computing can potentially reduce the time required to price these instruments, leading to more accurate and timely valuations.

Market Impact: Improved pricing models can lead to better market stability and more efficient financial markets.

7. Artificial Intelligence:

Enhanced Algorithms

Quantum Speedup: Quantum algorithms can potentially provide speedups for various AI tasks, including optimization, pattern recognition, and data classification, enabling more advanced AI systems.

Pattern Recognition: Quantum computing can enhance the accuracy and efficiency of pattern recognition tasks, which are essential in fields like image and speech recognition

Improved Data Handling

Large Datasets: Quantum computing can manage and process large datasets more efficiently, making it possible to analyze data that is currently unmanageable with classical systems.

Real-Time Analysis: Enables real-time data analysis for applications such as fraud detection, predictive maintenance, and dynamic pricing.

8. Climate Modeling

Weather Forecasting

Complex Models: Weather and climate models involve numerous variables and equations. Quantum computers can handle these complex models more accurately, leading to better short-term weather forecasts and long-term climate predictions.

Long-Term Predictions: Improved climate simulations can provide better insights into climate change and its potential impacts, aiding in policy-making and mitigation strategies.

Environmental Simulations

Ecosystem Modeling: Quantum computing can simulate complex ecological systems, helping scientists understand the interactions between different species and their environments.

Conservation Efforts: Detailed simulations can assist in designing effective conservation strategies by predicting the impact of environmental changes on ecosystems.

9. Logistics and Transportation:

Route Optimization

Efficient Routing: Quantum algorithms can find optimal transportation routes, reducing travel time, fuel consumption, and operational costs. This is valuable for logistics companies looking to maximize efficiency.

Logistics Planning: Enhances logistics planning by optimizing delivery routes and schedules, leading to cost savings and improved service levels.

Traffic Flow Management

Real-Time Data: Quantum computing can analyze real-time traffic data to optimize traffic flow, reducing congestion and improving travel times. This can lead to more efficient urban transportation systems.

Urban Planning: Assists in urban planning by providing detailed simulations of traffic patterns and potential improvements, helping cities design better infrastructure.

10. Cybersecurity

Post-Quantum Cryptography

Resilient Algorithms: As quantum computers become capable of breaking current cryptographic systems, there is a need to develop new cryptographic algorithms that are secure against quantum attacks. These algorithms are being standardized to ensure future-proof security.

Standardization: Organizations like NIST are working on standardizing post-quantum cryptographic algorithms to ensure they are widely adopted and implemented before quantum computers pose a real threat.

Secure Communications

VII. CONCLUSION

Utilizing the concepts of superposition and entanglement found in quantum mechanics, quantum computing represents a fundamental change in the way humans handle information. For some applications, it can do calculations that are significantly more complex than those possible with classical computers. Despite being in its infancy, the field has already demonstrated enormous promise in resolving challenging issues in materials research, drug development, cryptography, and optimization. But there are still a number of important issues to be resolved, such as scalability, error rates, and qubit stability. Overcoming these challenges and creating workable, large-scale quantum systems will be necessary for the advancement of quantum computing.

In conclusion, even though quantum computing holds out the possibility of revolutionary breakthroughs, more research is still needed to fully grasp the technology's potential and successfully incorporate it into practical uses.

REFERENCES

- [1] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, et al., "Superconducting quantum circuits at the surface code threshold for fault tolerance", *Nature*, vol. 508, no. 7497, pp. 500-503, 7497.
- [2] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe and S. Lloyd, "Quantum machine learning", *Nature*, vol. 549, no. 7671, pp. 195-202, 7671.
- [3] S. Debnath, N. M. Linke, C. Figgatt, K. A. Landsman, K. Wright and C. Monroe, "Demonstration of a small programmable quantum computer with atomic qubits", *Nature*, vol. 536, no. 7614, pp. 63-66, Aug. 2016.
- [4] N. Ofek, A. Petrenko, R. Heeres, P. Reinhold, Z. Leghtas, B. Vlastakis, et al., "Extending the lifetime of a quantum bit with error correction in superconducting circuits", *Nature*, vol. 536, no. 7617, pp. 441-445, Aug. 2016.
- [5] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM Rev.*, vol. 41, no. 2, pp. 303-332, Jan. 1999.
- [6] L. G. S. Imre, *Advanced Quantum Communications: An Engineering Approach*, Hoboken, NJ, USA: Wiley, 2013
- [7] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Commun. ACM*, vol. 21, no. 2, pp. 120-126, Feb. 1978.
- [8] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484-1509, 1997, [online].
- [9] I. L. Chuang, R. Laflamme, P. W. Shor and W. H. Zurek, "Quantum computers factoring and decoherence", *Science*, vol. 270, no. 5242, pp. 1633-1635, Dec. 1995.
- [10] W. G. Unruh, "Maintaining coherence in quantum computers", *Phys. Rev. A Gen. Phys.*, vol. 51, no. 2, pp. 992-997, Feb. 1995.
- [11] B. Georgeot and D. L. Shepelyansky, "Quantum chaos border for quantum computing", *Phys. Rev. E Stat. Phys. Plasmas Fluids Relat. Interdiscip.*

[12] G. Kalai, "The argument against quantum computers" in Quantum Probability Logic: The Work and Influence of Itamar Pitowsky, Springer, pp. 399-422, 2020.