IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, March 2026
Impact Factor: 8.2

Quantum Computing : Fundamental Principles, Quantum Algorithms, and Emerging Applications

Koteswararao P[1*], Dr. G. Vishnumurthy[2], P.Varalaxmi[3], T. Lohithsrinivas[4], K. S Siva Rama Krishnan[5]

[1]Department of Physics, ACE Engineering College, Hyderabad, India
[2]Department of CSE, Anurag University, Hyderabad, Telangana, India
3Department of Physics, Anurag University, Hyderabad, Telangana, India
[4,5]Department of Mechanical Engineering, ACE Engineering College, Hyderabad, India
koteswarphd@gmail.com

Abstract: *Quantum computing is an emerging computational paradigm that leverages fundamental principles of quantum mechanics, including superposition and entanglement, to perform computations beyond the capabilities of classical computers. Unlike classical bits, quantum bits (qubits) can exist in multiple states simultaneously, enabling exponential computational advantages for specific classes of problems. This paper presents the fundamental distinctions between classical and quantum computation, emphasizing qubit operational principles, quantum processing methods, and quantum gate operations. Key quantum algorithms, including Shor's algorithm, Deutsch–Jozsa algorithm, and Grover's search algorithm, are analyzed to demonstrate the computational superiority of quantum systems. Furthermore, major implementation challenges and diverse application domains of quantum computing are discussed*

Keywords: Quantum computing, qubits, quantum gates, quantum algorithms, superposition, entanglement

I. INTRODUCTION

Today's computers are smaller, cheaper, faster, greatly efficient, and even more powerful when we compare with early computers that used to be huge, costly, and more power-consuming. It becomes possible due to improvements in architecture, hardware components, small transistors and software running on them. Electronic circuits used in computers are getting smaller and smaller day by day. Transistors are small semiconductor devices that are used to amplify and also switch electric or electronic signals. They were used to be fabricated on a piece of silicon. The circuit was made by connecting these transistors together into a single silicon surface. The shape of circuits in an IC was printed together in all layers of silicon at the same time. This process takes the same amount of time even if the number of transistors in the circuit was increased. The cost of production of IC was decided by the size of silicon and not the number of transistors. This reduced the price of products due to which manufacturing and selling of IC increased and thus benefits and sales also. From the idea of connecting individual transistors to the collection of these transistors (Logic Gates) and finally, the collection of these Logic Gates used to get connected into a single integrated circuit (IC). Nowadays, a single IC can even integrate small computers onto it. The pursuit of computational speed and efficiency has driven innovation for decades. As Moore's law approaches its physical limits, classical computing architectures face challenges in energy efficiency, miniaturization, and data handling. This leads to the idea of the smallest computer by reducing the size of the circuit up to the size of an atom. But then these circuits will not be able to act as a switch as electrons inside an atom can become invisible from one side of a barrier and appear on another side, i.e. they can exist in more than one place at the same time. This is due to the teleporting phenomena in quantum mechanics called "Quantum Tunnelling". Quantum computing (QC) emerges as a transformative technology that exploits *superposition*, *entanglement*, and *quantum interference* to achieve computational capabilities beyond classical limits and exponential

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, March 2026
Impact Factor: 8.2

speedups for specific classes of problems, such as integer factorization, database search, and quantum simulation.The concept of quantum computation emerged in the late twentieth century as researchers began to recognize the computational implications of quantum mechanics. Charles Babbage often called the "Father of the computers". He created (or) discovered first mechanical computer in 1830. In the early 1980s, Richard Feynman proposed that classical computers face intrinsic limitations in efficiently simulating quantum systems, suggesting that quantum mechanical systems themselves could serve as computational devices. Building on this idea, David Deutsch introduced the model of a universal quantum computer, thereby providing a formal theoretical framework for quantum algorithms and quantum information processing.In this paper, we mainly discuss the fundamentals of classical and quantum computers,principles of quantum mechanics, quantum information processing,various algorithms, applicationsand associated[1-4].

II. PRINCIPLES OF QUANTUM MECHANICS

2.1.Super position and entanglement

Due to superposition more than one qubit state exists simultaneously. Fundamental unit of computer is qubits. These qubits may exist either 0,1 or both simultaneously.

Ex: Superposition can be explained by using bulb anology if it is ON state represents 1 and the OFF state represents 0. A dimly glowing bulb indicates combination of both states representing superposition state[5].

Entanglement is correlation between two qubits in quantum system. It is an integral part of quantum mechanics. Then one can notice that if any particle or qubit is subject to change; correspondingly the effect can be noticed on all the particles no matter what their distance of separation is. This principle is also used highly at the time of processing in the quantum computers. Entanglement between qubits helps process the information faster[6].

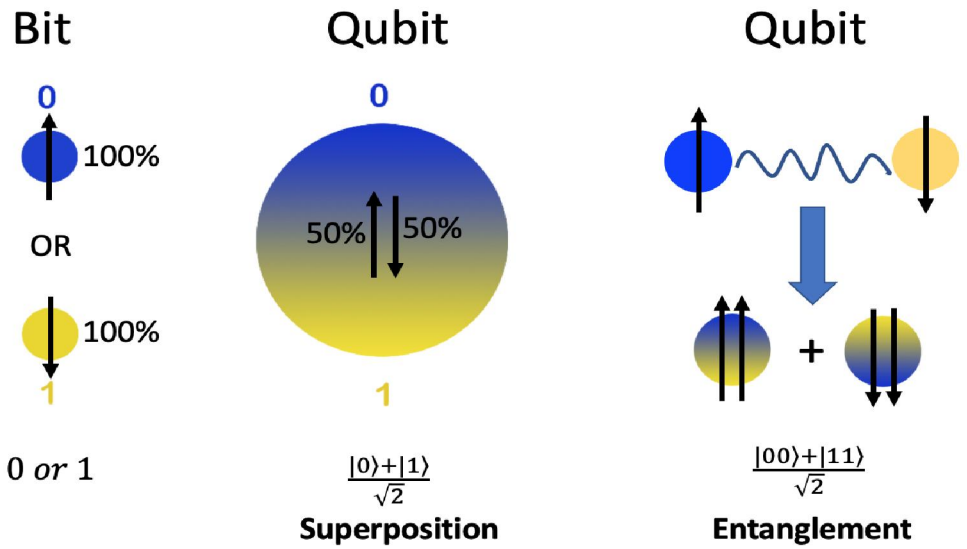

Fig.1.Illustrates the phenomenon of Super position quantum entanglement between two qubits[6]

2.2 Coherence: A quantum system is said to be coherent when it's state can be described using a set of complex numbers because each number representing the different base states of the system and It allows to maintain a fixed relationship that is the particles exhibiting coherence will demonstrate a specific behaviour when exposed to the circumstances of the surroundings [5-6].It is an important for particle can be entangled or show super positioning only.

2.3 Probability principle: According to max Born in 1926, Probability density must equal to 1.

It represents that the probability of obtaining any possible measurement's outcome is equal to square of corresponding amplitude[7].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, March 2026
Impact Factor: 8.2

2.4 Building blocks:

Classical computer it works on bits but quantum computer works using qubits and qubit (quantum bit) is the analogous concept for quantum computation and quantum information. It can exhibit the principles of superposition, entanglement which allows us for higher parallelism and faster computation. While a bit exists as either 0 or 1, a qubit can exist in a linear combination of both states simultaneously: These qubits are mostly represented using wave functions since the quantum computers obey the laws of schrödinger wave equations

A general qubit is represented as:

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

where α and β are complex probability amplitudes.

The normalization condition requires that the sum of the squared absolute values of these amplitudes equals one:

$$|\alpha|^2+|\beta|^2=1.$$

When a qubit is measured, the probability of obtaining outcome 0 is $|\alpha|2$, and the probability of obtaining outcome 1 is $|\beta|^2$. This probabilistic result is known as Born's rule.

To visualize qubits, we use the Bloch sphere. The Bloch sphere is a three-dimensional representation where each point on its surface corresponds to a possible state of a qubit.[8]

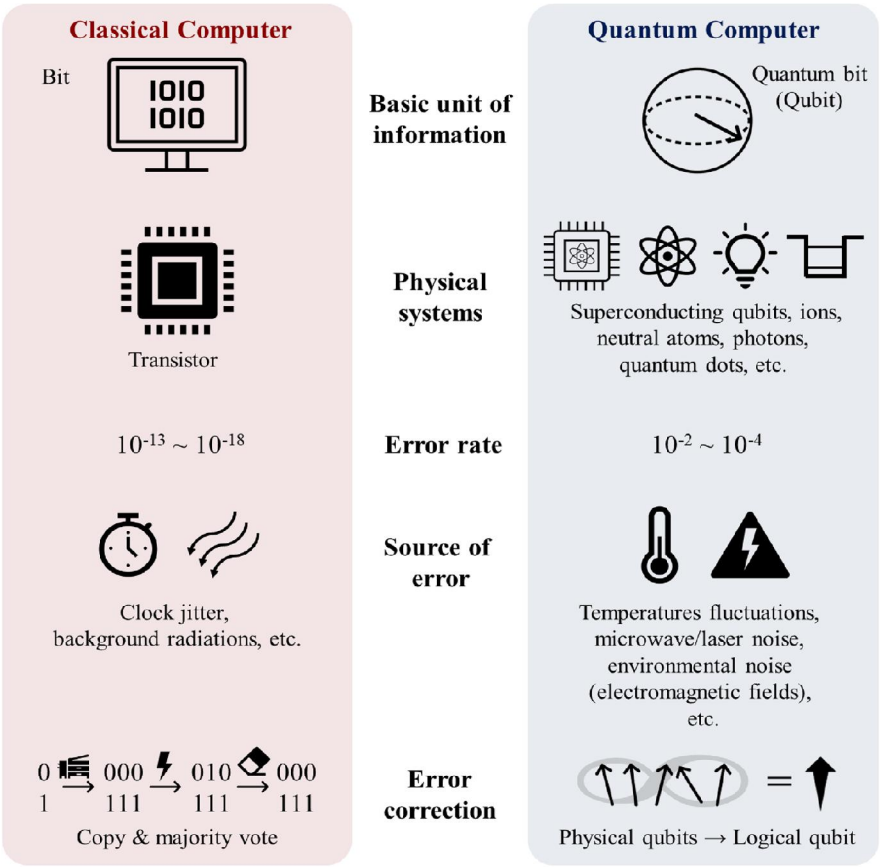

Fig2: Difference between classical and quantum computer[8]

III. QUANTUM COMPUTING FOR INFORMATION PROCESSING

Quantum computing uses principles of quantum mechanics—like superposition, entanglement, and interference—to process information in ways that are fundamentally different and, for certain problems, exponentially more powerful

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, March 2026
Impact Factor: 8.2

than classical computers. Instead of binary bits (0 and 1)quantum computer uses qubits which can exist in multiple states at a time.[8]

Table 1. Physical Representation of Quantum Computers:

S. No.	Method	Qubit / Use	Operation Principle	Ref.
1	Ion Trap Quantum Computing	Individual trapped ions as qubits	Ions confined by electromagnetic fields; quantum states manipulated using laser beams	[9]
2	Superconducting Quantum Computing	Superconducting circuit qubits	Superconducting circuits at very low temperature; qubits controlled using microwave pulses	[10]
3	Linear Optical Quantum Computing	Photons as qubits	Photons processed through linear optical elements (beam splitters, phase shifters, detectors)	[11]
4	Semiconductor Spin-Based Quantum Computing	Electron spin in semiconductors (e.g., silicon)	Spin states in quantum dots or doped silicon manipulated electrically/magnetically	[9]
5	Nuclear Magnetic Resonance (NMR) Quantum Computing	Nuclear spins of molecules	Nuclear spins controlled using magnetic fields and radio-frequency pulses	[9]
6	Quantum Computing with Defects	Defect centers (e.g., NV centers in diamond, SiC vacancies)	Electron or nuclear spin of defect manipulated using optical/microwave fields	[12]

IV. FAMOUS ALGORITHMS

Since in this quantum era from olden days to modern days different types of algorithms are been introduce by scientists. These algorithms are used widely because to find out the solutions for complex problems. Such as finding the element or data from unsorted databases; factorizing large numbers; to find out whether the function is constant or balanced. There are three main key algorithms such as “Shor’s algorithm’’, “Grovers algorithm” and “Deutsch-Jozsa algorithm”. These algorithms are mostly used to solve certain complex problems. These algorithms give a exponential speedup than classical systems [13].

4.1 Shor’s algorithm

Peter Shor introduced “Shor algorithm” in 1994 As Shor algorithm was popular in quantumcomputation because Shor algorithm can efficiently factors large integers into their prime factors. Providing a breaking solution to complex problems. Has classical computers where failed to solve the problems of large integers. this gives a significant speedup over classical systems and running in polynomial time instead of exponential time.

The Breathe of Shor’s algorithm is to identify the period “r” of the function. Such that f(x)=a*mod N, where N is a integer to be factorized , a is a random chosen number In this process superposition plays a key role to perform multiple calculations at the same time. Such that helps to determine period. This step is required for breaking down the large integers into their prime factors. Once it we get the value of “r”. The next step is GCD which is applied to it. Calculating the factors using GCD of “$a^{\frac{r}{2}} - 1 \; and \; a^{\frac{r}{2}} + 1$”. By which it reduces the large numbers into their prime factors. In case if r is invalid then again choose a random value of (a). Shor’s algorithm has major implications for cryptography and security of many systems like RSA encryptions [13-15].

4.2 Grover’s Algorithm.

Grover’s algorithm was discovered by Lov Grover in 1996 (25). It is a method of searching unsorted database.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, March 2026 Impact Factor: 8.2

It searches the required data or element in O(N) time (26). Such that O($\sqrt{N}$) trials are required; To find out the required element or target (27).Suppose we have some unsorted data and we are trying to find out the f(x) from the data such that we have N=2^n elements.

Let us separate the target elements and remaining elements in terms of

$$\Psi\_0 = \alpha\_0 \mid r\rangle + \beta\_0 \mid t\rangle$$

Hence initially both are having same amplitude. Such that we have to increase the amplitude of the target element the rest of elements amplitude decreases. Due to the same initial amplitudes the superposition lie's in between the target element and remaining elements. Then the inversions and diffusion operators are applied to relatively increase the amplitude of the target elements. This process will repeat up to N times, to increase the amplitude of the correct element (target)[16-17].

$$\Psi\_0 = \alpha\_\{n\}\sum\_\{r \neq t\}\^\{\} \mid r\rangle + \beta\_n \mid t\rangle$$

Apply the normalization condition we get $r = O\sqrt{N}$.

4.3 Deutsch-Jozsa Algorithm

The Deutsch-Jozsa algorithm was invented by David and Jozsa in 1992 [22]. This algorithm helps to determine whether the give is balanced or constant. In case of constant, it gives same output but in case of balanced half is zero and another half is one. So almost 0's and 1's are equal. It solves the complex problems in one query by exponential speedup.

Let us consider a function f(x) such that to check whether it is balanced or constant. Consider unitary operators. (n/) notations. By applying the phase kick back conditions and quantum parallelism conditions we get

$$⍁\{1\}\{N\}\sum\_\{z = 0\}\^\{N - 1\} \vdash [\sum\_\{x = 0\}\^\{N - 1\} \vdash (-1 \dashv)\^\{f \vdash (x \dashv)\} \vdash (-1 \dashv)\^\{x.z\} \dashv] \mid z\rangle\_n \mid -\rangle$$

Assume amplitude of Ket z is zero then, we get

$$\frac{1}{N}\sum_{x=0}^{N-1}(-1)^{f(x)}$$

In case of constants f(x)=f(1) =0 or f (0) =f (1) =1 and in case of balanced f (0) =0,f (1) =1 or f (0) =1, f (1) =0 after all possible checks; measurements will arise the correct answers (13).

V. APPLICATION OF QUANTUM COMPUTER

Quantum computing offers potential breakthroughs in areas where classical computers are limited by the computational complexity of problems with many variables.

Materials science and chemistry: Quantum computers can simulate molecular behavior and chemical reactions with high accuracy. This can accelerate the discovery of new drug candidates, optimize catalysts for chemical reactions, and help design advanced materials, such as improved batteries and superconductors. [23]

Cryptography and security: While quantum computers could break today's standard encryption (like RSA) using Shor's algorithm, they also offer the solution. Quantum Key Distribution (QKD) provides an un-hackable way to exchange keys, and the development of post-quantum cryptography (PQC) focuses on new, quantum-resistant encryption methods. [24]

Machine learning and artificial intelligence: Quantum computing can provide an exponential or quadratic speedup for certain machine learning tasks, such as training models, speeding up pattern recognition, and analysing large datasets. [25]

Optimization: Quantum algorithms are designed to find the optimal solution from a vast number of possibilities. This has applications in logistics, such as optimizing traffic flow and supply chains, and in finance, for portfolio optimization and fraud detection.[26]

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, March 2026 Impact Factor: 8.2

Simulation: The ability to simulate complex systems is invaluable for fields like climate modelling and weather forecasting. Quantum computing can process the multitude of variables involved more efficiently, leading to more accurate predictions[27]

Overall Advantages

Quantum algorithms are used to solve the complex problems of the linear system and optimizations. Key algorithms like shor's algorithm which is used to solve the large integers into their prime factors. Grovers algorithm is used to find an element from the unsorted databases. These algorithms offer an quadratic speed up than classical computers. Whereas superposition helps for multitasking. Quantum parallelism helps the superposition to act at a time in different places to find out the solutions. At present the systems are developing and almost reducing the error rates by increasing the number of qubits. The primary advantage of quantum computer is present in the ability of leverage quantum mechanics principles [28-29].

Overall challenges

There are a lot of benefits in quantum computers and at the same time there are some challenges from olden daysto the modern days. Such as error correction; wherelarge codes are been used to correct the errors but it also increases some other errors. Large scale of error correction is required to bring out the potential of the quantum computers to the application perspective. Which can reduce the errors. The user should easily access the quantum computers without any noise. The scalability of qubits should be increased to solve the complex problems faster. Making sure to advance the theory of quantum computation to bring some new insights. Decoherence is also a challenge such that calculations must be done before the decoherence occurs.[30].

REFERENCES

[1] Copeland, B. J. (2000). The modern history of computing, https://plato.stanford.edu/entries/computing-history/

[2] Theis, T. N., & Wong, H. S. P.(2017). The end of moore's law: A new beginning for information technology. *Computing in Science & Engineering*,*19*(2), 41-50.

[3] Richard P. Feynman, "Simulating physics with computers (1982)," International Journal of Theoretical Physics, Vol. 21, Nos. 6/7.

[4] Igor YaDoskoch, Superposition Principle and Born's Rule in the Probability Representation of Quantum States, Lebedev Physical Institue, Moscow, 2019.

[5]Rietsche, R., Dremel, C.,&Bosch, S. (2022).Quantum computing. *Electronic Markets, 32*, 2525-2536. https://doi.org/10.1007/s12525-022-00608-y.

[6]Gühne, O., & Tóth, G. (2009). Entanglement detection. *Physics Reports, 474*(1-6), 1-75.

[7] Chae, E., Choi, J., & Kim, J. (2024). An elementary review on basic principles and developments of qubits for quantum computing. *Nano Convergence*, *11*(1), 11. https://doi.org/10.1186/s40580-024-00418-5.[8]

[9] Bhat, H.A.; Khanday, F.A.; Kaushik, B.K.; Bashir, F.; Shah, K.A. Quantum Computing: Fundamentals, Implementations and Applications. IEEE Open J. Nanotechnol. 2022, 3, 61–77.

[10]Hassija, V.; Chamola, V.; Saxena, V.; Chanana, V.; Parashari, P.; Mumtaz, S.; Guizani, M. Present Landscape of QuantumComputing. IET Quantum Commun. 2020, 1, 1.

[11] Nandhini, S.; Singh, H.; Akash, U.N. An extensive review on quantum computers. Adv. Eng. Softw. 2022, 174, 103337.

[12]Hughes, C., Isaacson, J., Perry, A., Sun, R.F., & Turner, J. (2021). What is a qubit?. In *Quantum Computing for the Quantum Curious* (pp. 7-16). Springer International Publishing. https://doi.org/10.1007/978-3-030-61601-4_2.

[13]Ansh Chawla, Sankalp Mathur, Harshit Rao,Naman Mudgal, Anita BhardwajQuantum Computing-The Underlying Principle Behind it,Vol. 4, No. 2, 235-258, 2025.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, March 2026 Impact Factor: 8.2

[14]Willsch, D., Willsch, M., Jin, F., De Raedt, H., & Michielsen, K. (2023). Large-scale simulation of Shor's quantum factoring algorithm. Mathematics, 11(19), 4222.
[15] Peter W. Shor†,Polynomial-Time Algorithms for Prime Factorizationand Discrete Logarithms on a Quantum Computer, 25 Jan 1996.
[16] Kumar, M., & Mondal, B. (2024). Study on implementation of Shor's factorization algorithm on quantum computer. SN Computer Science, 5(4), 413
[17]Shor, P.W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review, 41(2), 303-332
[18]Gerjuoy, E. (2005). Shor's factoring algorithm and modern cryptography: an illustration of the capabilities inherent in quantum computers. American Journal of Physics, 73(6), 521-540.
[19] Kulkarni, S.S., & Thakar, H.S. (2024). Quantum cryptanalysis: analyzing Shor's algorithm and its impact on RSA. In Proceedings of 5th International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications (Vol. 1, p. 347). Springer Nature. Singapore.
[20] Singh, S., & Sakk, E. (2024). Implementation and analysis of Shor's algorithm to break RSAcryptosystem security. 3.grovers algorithm
[21] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (pp. 212-219). Association for Computing Machinery. New york.
[22]Hooyberghs, J. (2022). Deutsch-Jozsa algorithm. In Introducing Microsoft Quantum Computing for Developers. Apress, Berkeley, CA.
[23] Cao, Y., Romero, J., &Aspuru-Guzik, A. (2018). Potential of quantum computing for drug discovery. *IBM Journal of Research and Development, 62*(6), 6-20.
[24]Nielsen, M., & Chuang, I. (2010). *Quantum computation and quantum information*. Cambridge University Press. UK.
Egger, D.J., Gambrell, C., Marecek, J., McFaddin, S., Mevissen, M., Raymond, R., &Yndurain, E. (2020). Quantum computing for finance: state-of-the-art and future prospects. *IEEE Transactions on Quantum Engineering*, *1*, 1-24.
[25]Farhi, E., Goldstone, J., & Gutmann, S. (2014). *A quantum approximate optimization algorithm applied to a bounded occurrence constraint problem*. arXiv:1412.6062.
[26]Kimble, H.J. (2008). The quantum internet. *Nature, 453*(7198), 1023-1030.
[27]Yan Wang, Jungin E. Kim, Krishnan SureshOpportunities and Challenges of Quantum Computing for Engineering OptimizationComput. Inf. Sci. Eng. Dec 2023, 23(6): 060817
[28]Travis L. Scholten∗1, Carl J. Williams2, Dustin Moody3, Michele Mosca4,5,6, William"whurley" Hurley7, William J. Zeng8,9, Matthias Troyer10, and Jay M. Gambetta1Assessing the Benefits and Risks of Quantum Computers, 13 Feb 2024.
[29]Peter W. Shor,Polynomial-Time Algorithms for Prime Factorizationand Discrete Logarithms on a Quantum Computer, 25 Jan 1996.
[30]I. L. CHUANG, R. LAFLAMME, P. W. SHOR, AND W. H. ZUREK, Quantum Computers, Factoring, and Decoherence8 Dec 1995Vol 270, Issue 5242pp. 1633-1635.