QUANTUM COMPUTING: TERMINOLOGY, APPLICATIONS, SECURITY AND BEYOND

Karimov Madjit Malikovich

Agency for Assessment of knowledge and competences under the ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan, Tashkent, Uzbekistan
dr.mmkarimov@rambler.ru

Komil Tashev

Department of Cryptology,
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan.
k.akhmatovich@gmail.com

Nuriddin Safoev

Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

Abstract. *Quantum computing diverges from classical computing by leveraging principles rooted in quantum mechanics, making use of distinctive features such as entanglement and superposition. The pivotal distinction between a quantum computer and its classical counterpart lies in its remarkable capacity to process information at an exceptionally accelerated rate, a capability facilitated by the concept of quantum entanglement. Interest in the phenomenon of quantum entanglement has experienced exponential growth in recent years, with the past decade witnessing notable advancements in the practical implementation of quantum computation within the realm of quantum information. This investigation systematically curated secondary resources from various databases spanning nearly a century, employing specific keywords. The ensuing presentation encapsulates the fundamentals of quantum computing, its applications, and the pivotal role played by quantum entanglement. Consequently, this research contributes to a comprehensive understanding of quantum computing, its applications, and the significance of quantum entanglement in the field.*

Keywords: *quantum computing; quantum entanglement; quantum state; technological revolution; quantum industry applications.*

1. Introduction

In 1935, the Einstein-Podolsky-Rosen (EPR) Paradox, a thought experiment exploring a novel and intriguing phenomenon, was formulated by Einstein, Podolsky, and Rosen [1]. Following this, Schrödinger delved into the concept of quantum entanglement inspired by the EPR Paradox. Even Schrödinger found it challenging to comprehend how this concept violated the theory of relativity [2]. By 1964, Bell demonstrated that quantum entanglement contradicts classical mechanics' attributes, challenging realism, locality, and completeness, adhering exclusively to the principles of quantum mechanics [3]. Although the concept of quantum entanglement was established, its recognition remained limited until the exploration of its applications and understanding of its pivotal role.

Quantum entanglement stands as the cornerstone of quantum mechanics [4], presenting a peculiar physical phenomenon wherein the states of entangled objects automatically correlate, regardless of the spatial separation between them. This phenomenon has become a crucial asset in the realm of quantum information [5], playing a fundamental role in quantum information processing. Its applications extend to various domains, including quantum computing, quantum teleportation, and quantum cryptography. Furthermore, it serves as a key element in enabling quantum computers to surpass classical computers in computing capabilities [6]. The surge in interest in quantum entanglement over recent decades has paralleled significant strides in quantum computing [7].

In 2021, IBM unveiled the "Eagle" quantum computing chip, housing 127 quantum bits (qubits), marking a noteworthy advancement in quantum computing [8]. Subsequently, in 2022, IBM introduced 'Osprey,' featuring 433 qubits, setting a record for the highest number achieved in a quantum processor. Anticipated for the end of 2023, IBM's 'Condor' is poised to be the first quantum processor surpassing 1,000 qubits. A comprehensive grasp of the fundamentals of quantum computing and entanglement is imperative for navigating the evolving landscape of quantum technology. This paper seeks to provide a broad understanding of quantum computing, its applications, and the pivotal role of quantum entanglement in this context.

2. Quantum Computing

2.1. Quantum entanglement

Quantum entanglement is a phenomenon wherein the quantum states of multiple subsystems cannot be independently described, even when the distance between these

subsystems is considerable [9]. To simplify this concept, consider two coins, one labeled "head" and the other "tail" on both sides. Each coin is given to two individuals, Alice and Bob, who are separated by a significant distance—Alice on Earth and Bob on Mars. They are informed that the coin they possess must be either a "head" or a "tail." In this classical scenario, their coins are correlated and entangled. Let's assume both Alice and Bob reach their respective destinations. Upon observing her coin, if Alice discovers it to be a "head," she simultaneously knows that Bob's coin must be a "tail." This logical sequence contradicts classical mechanics and aligns with the principles of quantum mechanics.

A quantum bit, or qubit, serves as the fundamental unit for carrying information in quantum computing [10]. To simplify, in classical computing, a bit represents information as either 0 or 1. In contrast, a quantum computer utilizes qubits to represent information.

2.2. Quantum computer vs classical computer

The proposition of a quantum computer aims to simulate processes beyond the reach of classical computers [11,12], presenting an unparalleled paradigm for information processing [13]. Quantum computers leverage the collective attributes of quantum states, including superposition, interference, and entanglement, in accordance with the principles of quantum mechanics. This stands in stark contrast to classical computers, which adhere to the principles of classical physics.

While both classical and quantum computers can address some similar computational problems, the primary distinction lies in the time required to solve certain computational issues [12]. Notably, the incorporation of the quantum entanglement principle in quantum computers significantly amplifies processing speed [14]. As indicated by [4], augmenting the number of qubits or creating more extensive entangled states further enhances the processing speed of quantum computers. Numerous other distinctions between classical and quantum computers are outlined in Table 1 for clarity.

Table 1. The differences between classical and quantum computer.

CLASSICAL COMPUTER	QUANTUM COMPUTER
Governed by classical physics principles	Governed by quantum mechanics
Large scale integrated multi-purpose computer (CPU)	High speed parallel computer based on quantum mechanics
Boolean logic operations	Quantum gate operations or energy state manipulation
Gates run forward	Gates are reversible
Use bit to represent information	Use qubit or quantum bit to represent information
Information storage is bit based on voltage/charge	Qubit based on direction of an electron spin
Low rates of error	High rates of error
Operate at room temperature	Operate at extremely cold temperature
Minimal inherent noise	Extremely sensitive to noise
Circuit behavior is governed by classical physics	Circuit behavior is governed explicitly by quantum mechanics
No restriction on copying and measuring signals	Uncompromising restriction on copying and measuring signals

Quantum computers are rapidly advancing, gaining momentum over the years and posing a potential challenge to the continued dominance of classical computers, particularly in addressing problems with a vast number of variables and potential outcomes. Despite the potential threat to classical computing, this progress also brings about significant opportunities across various disciplines in the modern era.

2.3. Applications of quantum computing

Cloud-based quantum computing services have been introduced and applied in diverse fields, including education, research, and gaming. These services offer a pathway to quantum computing by providing a publicly accessible quantum computing platform in a cloud environment. This platform is available to users worldwide, allowing them to perform authentic quantum processing tasks [15]. For an overview of some existing cloud-based quantum computing platforms, refer to Table 2.

Table 2. The existing cloud-based quantum computing platforms.

COMPANY PRODUCT	SOURCE	DESCRIPTION
Forest (Rigetti Computing)	www.rigetti.com	A quantum programming toolkit
Microsoft Azure Quantum (Microsoft)	www.azure.microsoft.com	A quantum system and toolkit for quantum computing
IBM Q Experience (IBM)	www.quantum-computing.ibm.com	A quantum system, simulators, and programming tools
Quantum Playground (Google)	www.quantumplayground.net	A quantum simulator and 3D quantum state visualization
Quantum Inspire (Qutech)	www.quantum-inspire.com	A quantum computing platform provides a fully programmable 2-qubit electron spin quantum processor and a 5-qubit transmon processor
FORGE (QC WARE)	https://forge.qcware.com/	provides access to D-Wave hardware as well as Google and IBM simulators
D-WAVE	https://www.dwavesys.com/	
Amazon Bracket (Amazon)	www.aws.amazon.com/braket	A quantum simulator that can be run on different quantum hardware technologies
Xanadu Quantum Cloud (Xanadu)	www.xanadu.ai/cloud	A photonic quantum computing platform

Quantum computing is poised to revolutionize numerous industries in the future, as predicted by IBM across three horizons in the industrial revolution [16]. The transformative potential of quantum computing technology extends across various sectors. In healthcare and life sciences, for instance, collaborations between oncologists, physicists, and computer scientists at the German Cancer Research Center aim to leverage quantum computing for classifying and selecting specific therapies from diverse datasets, potentially benefiting cancer patients [17]. Similarly, the renewable energy sector recognizes the importance of quantum computing in addressing critical challenges related to renewable energy problems [18]. The

multifaceted impact of quantum computing is indicative of its potential to bring about significant advancements in various industries.

2.4. Data Security and Quantum Cryptography

Ensuring data security is imperative to safeguard critical information such as files, databases, accounts, and networks. In the contemporary digital technology era, effective data security is essential for both public and private sector organizations, given the potentially severe consequences of data breaches. The field of cybersecurity has gained increasing significance due to the growing reliance on computer systems and technological advancements. Over the years, cybersecurity has evolved alongside its counterpart, cyber threats, with continuous improvements implemented by experts. Cryptography serves as a crucial tool employed by cybersecurity experts to design algorithms and other measures aimed at protecting data.

Classical cryptography relies on computational mathematics, whereas quantum cryptography is rooted in the principles of physics, specifically following the laws of quantum mechanics, to secure the transmission of private information [19]. Table 3 outlines some key distinctions between classical and quantum cryptography.

Table 3. The differences between classical and quantum cryptography.

CLASSICAL CRYPTOGRAPHY	QUANTUM CRYPTOGRAPHY
Based on mathematical computation	Based on quantum mechanics
Widely used	Sophisticated
Digital signature is present	Digital signature is absent
Bit rate depends on computational power	Average bit rate is 1 Mbps
Deployed and tested	In initial stages, not fully tested
Low cost	High cost

Table 3 highlights several distinctions between classical and quantum cryptography. Classical cryptography relies on two primary methods—secret key (symmetric) cryptography and public key (asymmetric) cryptography. In contrast, quantum cryptography employs quantum key distribution (QKD), utilizing a series of photons and a qubit sequence to transmit the code between two ends. By comparing measurements of the properties of these photons, the communicating ends can establish a secure key for encrypting and decrypting information. Any disruption to the qubit sequence is detectable by both the sender and receiver, prompting the generation of a new bit sequence.

The ascent of quantum computing introduces vulnerabilities in classical encryption, but it also ushers in a new era of quantum-enhanced security protocols. Striking a balance between emerging threats and opportunities, the cryptographic landscape is on the brink of profound transformations in the quantum age. Close collaboration among businesses, policymakers, and technologists is paramount to ensuring the security of our digital world amidst the advancements in quantum technology.

3. Limitations of the Research

The rapid advancement in the field of quantum computing may have led to substantial developments in quantum hardware, algorithms, and applications that are not comprehensively covered in this paper. Quantum mechanics is a complex and abstract field. Conveying quantum concepts and their business implications in a concise and accessible manner poses a challenge. Some sections of the article may be demanding for readers without a background in quantum physics.

Limited Inclusion of Specific Business Cases: While the article explores potential applications of quantum computing across various industries, it may not delve into specific business cases or provide in-depth examples. The adoption of quantum technologies by businesses is expected to vary widely.

Space Constraints: Given the complexity and breadth of the topic, the paper may not cover every aspect of quantum computing's impact on society. Certain subtopics and nuances may be omitted or briefly summarized due to space constraints.

These limitations underscore the dynamic and evolving nature of the quantum computing field, the challenges in communicating complex concepts, and the speculative nature of predictions. Readers are encouraged to seek additional sources and updates to supplement their understanding of the rapidly advancing field of quantum computing.

4. Conclusions

In summary, this review has delved into the realm of quantum computing, exploring its applications and highlighting the pivotal role of quantum entanglement in enhancing processing speeds. The distinctions between quantum and classical computers were examined, with a specific emphasis on the integration of quantum entanglement as a key factor in the superior processing capabilities of quantum computers. The discussion also touched upon current applications of quantum computing.

Despite being in the early stages of development for commercial use, and acknowledging its existing limitations, quantum computing stands poised to bring

about transformative changes in the technological landscape. The potential impact of quantum computing on the broader technological world is substantial, making it a field of great promise and anticipation.

References

1. Einstein, A.; Podolsky, B.; Rosen, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.* **1935**, *47*, 777–780.

2. Schrödinger, E. (1935). Discussion of Probability Relations between Separated Systems. Mathematical Proceedings of the Cambridge Philosophical Society, 31(4), 555-563.

3. Bell, J. S. (1964). On the Einstein Podolsky Rosen paradox. Physics Physique Fizika,1(3), 195-200.

4. Yu, Y. (2021). Advancements in Applications of Quantum Entanglement. Journal of Physics: Conference Series, 2012(1), 012113.

5. Shi, X., Chen, L., & Hu, M. (2021). Multilinear monogamy relations for multiqubit states. Physical Review A, 104(1), 012426.

6. Mooney, G. J., Hill, C. D., & Hollenberg, L. C. L. (2019). Entanglement in a 20-Qubit Superconducting Quantum Computer. Scientific Reports, 9(1), 13465.

7. Wang, Y., Li, Y., Yin, Z.-Q., & Zeng, B. (2018). 16-qubit IBM universal quantum computer can be fully entangled. npj Quantum Information, 4, 1-6.

8. Ball, P. (2021). First quantum computer to pack 100 qubits enters crowded race. 599, 542.

9. Guo, Y. (2019). Introduction to quantum entanglement. AIP Conference Proceedings, 2066(1), 020009.

10. Erhard, M., Krenn, M., & Zeilinger, A. (2020). Advances in high-dimensional quantum entanglement. Nature Reviews Physics, 2(7), 365-381.

11. Maslov, D., Kim, J.-S., Bravyi, S., Yoder, T. J., & Sheldon, S. (2021). Quantum advantage for computations with limited space. Nature Physics, 17(8), 894-897.

12. Bravyi, S., Gosset, D., & König, R. (2018). Quantum advantage with shallow circuits. Science, 362(6412), 308-311.

13. Tura, J. (2021). Boosting simulation of quantum computers. Nature Computational Science, 1(10), 638-639.

14. Castelvecchi, D. (2017). Quantum computers ready to leap out of the lab in 2017. Nature, 541(7635), 9-10.

15. Almudever, C., Lao, L., Wille, R., & Guerreschi, G. G. (2020). Realizing Quantum Algorithms on Real Quantum Computing Devices.

16. Dilmegani, C. (2021). Top 20+ Quantum Computing Applications / Use Cases. Retrieved from https://research.aimultiple.com/quantum-computing-applications/

17. Abbott, A. (2021). Quantum computers to explore precision oncology. Nature Biotechnology, 39(11), 1324-1325.

18. Giani, A. (2021). Quantum computing opportunities in renewable energy. Nature Computational Science, 1(2), 90-91.

19. Upadhyay, L. (2019). Quantum Cryptography: A Survey, Cham.