2024 IEEE 67th International Midwest Symposium on Circuits and Systems (MWSCAS) | 979-8-3503-8717-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/MWSCAS60917.2024.10658839

Impacts of Quantum Mechanics: A Survey of Applied Quantum Computing

Dasheng Zhang, Eric Savage, Jin Feng Lin, Ruolin Zhou
Department of Electrical and Computer Engineering
University of Massachusetts, Dartmouth, MA

***Abstract*—In this survey paper, we provide an overview of the significance of quantum computing. It includes a review of fundamental principles, technological advancements, the interconnections, and reviews the current state of research, discussing both essential achievements and persistent challenges. The paper also examines how these technologies complement each other, enhancing secure communication and computational efficiency. We propose future research directions that emphasize the importance of further advancements to address existing challenges and optimize the utilization of quantum technologies across multiple sectors.**

I. Introduction

Quantum engineering technologies, especially quantum communication and quantum computing, are advancing the fields that impact scientific and technological landscapes [1]. For example, one of the potentials in quantum computing is to optimize energy grids with machine learning (ML), showing its application in distributed energy generation and transmission [2]. In the field of computer vision, quantum computing is recognized for its ability to tackle complex computational tasks more efficiently than classical methods. Additionally, the development of distributed quantum computing underscores its importance and promising applications in high-performance computing, highlighting its innovative impact on computational capabilities.

In this paper, we delve into the foundational concepts and trace their journey from theoretical notions to practical implementations, and provide a comprehensive overview of the current stage and the challenges faced.

The motivation for this work arises from transitioning from a theoretical background to practical applications, with a focus on assessing the feasibility of engineering applications of quantum technologies. By examining the current state of research, key achievements, and persistent challenges, this paper aims to provide insights into the potential real-world impact and practical deployment of quantum technologies.

The rest of the paper is organized as follows: Section II introduces quantum computing and its applications; Section III discusses impacts and future directions of quantum computing; and Section IV concludes the paper.

II. Quantum Computing and its Applications

Quantum computing harnesses quantum mechanics principles to process information. Its basic terminology is to channel quantum bits (qubits) to store data and compute. Unlike classical bits, qubits can exist in multiple states simultaneously due to superposition. Additionally, quantum entanglement allows quantum computers to perform complex calculations at speeds that far surpass those of classical computers. Quantum computing shows great promise in fields such as material science, drug discovery, and complex system simulations, potentially outperforming traditional computers in handling large datasets.

A. Physical Principle of Superposition and Entanglement

In quantum computing, the concept of basis states $|0\rangle$ and $|1\rangle$ can be analogously related to the boolean notation of 0 and 1 used in classical computing. The superposition state of a qubit is expressed as: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where $|0\rangle$ and $|1\rangle$ represent the fundamental binary states similar to classical bits, but with the quantum capability to exist in both states simultaneously. This duality allows quantum computers to perform complex parallel computations that are not feasible with classical systems. This relationship extends the binary logic into a quantum realm where the states are not exclusive but coexistent, enhancing computational efficiency and capability.

Quantum entanglement can be mathematically represented using the state vector notation in the Hilbert space. For instance, consider a simple system of two qubits that can be entangled. The entangled state can be expressed as: $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ Here, $|\Psi\rangle$ is the state vector of the entire system of two qubits, and $|00\rangle$ and $|11\rangle$ are basis states. The coefficient $\frac{1}{\sqrt{2}}$ ensures that the state vector is normalized.

B. Application in Communications

Quantum communication utilizes the principle of quantum mechanics. Entanglement and superposition are two primarily used principles, to enable secure information transfer. Quantum communication advances the data security, as using qubits in communication are highly sensitive to eavesdropping, which interfere the quantum state and can be immediately detected. One of the most profound applications of quantum communication is Quantum Key Distribution (QKD). This implementation is embedded in the quantum properties of particles, which cannot be measured without altering their state and, as a result, allows communication authorized users to generate and share a secure encryption key over a distance, potentially preventing the communication channel from all forms of eavesdropping.

Recent developments in QKD have focused on enhancing its performance and practicality. In addition to its applications in network security and data transmission, quantum communication can also be utilized in energy transmission and the creation of virtual communities. By using quantum optimization algorithms, the data transmission paths in energy grids can be optimized to enhance transmission efficiency and security. For instance, studies have shown that the application of quantum computing in load scheduling and microgrid formation can optimize current energy consumption and production, forming self-sufficient energy communities [2]. Advancement in satellite-based QKD have significantly extended the operational range beyond the limitations of terrestrial fiber networks [3]. This development allows for secure quantum communication across global distance, which is crucial for international data security. Experiments involving satellite QKD communication has proved the feasibility of implementation.

C. *Application in Cybersecurity*

Quantum computing significantly impacts cybersecurity by offering both innovative security solutions and new vulnerabilities. One of the major advantages is QKD, which uses quantum mechanics to ensure secure communication that is theoretically immune to hacking attempts. This technology guarantees that any attempt to intercept data changes the quantum states, making eavesdropping detectable. The change of quantum states yields the change of quantum information, which provides a false information for eavesdropper make receiver notice the existence of eavesdropper.

However, the rise of quantum computing also poses risks to conventional cryptographic systems that protect our digital transactions. Quantum algorithms, such as Shor's algorithm, could potentially decrypt many current cryptographic methods that depend on the complexity of tasks like factoring large numbers.

To counteract these threats, the field is moving towards developing quantum-resistant algorithms, also known as post-quantum cryptography. These new algorithms are designed to be secure against both traditional and quantum computational threats, ensuring robust protection as quantum technology evolves.

In addition, the field of quantum cybersecurity is not only focusing on data encryption, but is also exploring broader applications. Researchers are investigating how other quantum properties, such as entanglement and superposition, can be harnessed to enhance security protocols beyond encryption. This includes secure multi-party computation and quantum random number generation.

As quantum computing continues to grow, its integration into cybersecurity strategies will be crucial for defending against sophisticated cyber threats. Staying updated with the latest research and developments in quantum computing and cybersecurity is essential for professionals in the field to navigate this rapidly evolving landscape.

D. *Application in AI/ML*

Studies and reviews conclude the insights into applications of quantum computing in artificial intelligence and machine learning. Quantum machine learning (QML), specifically using variational quantum circuits (VQC) within the deep Q-Network (DQN) framework seeks to adapt classical reinforcement learning elements such as target networks and experience replay into quantum realm and utilizing the computational advantages of quantum systems [4]. QML potentially drives breakthroughs in computational tasks due to the intersection of quantum computing and classical machine learning [5]. These advantages include the capability to perform complex computations more efficiently than classical systems, which can lead to improvements in speed and performance for machine learning tasks. Moreover, QML is anticipated to handle computations that are challenging for classical computers, particularly in high-dimensional data environments where quantum properties like superposition and entanglement can be used to process information in fundamentally novel ways.

Quantum optimization algorithms, such as Quantum Approximate Optimization Algorithm (QAOA) and quantum annealing techniques, have shown great potential in addressing complex optimization problems. For instance, in smart grids, quantum optimization technologies are used for dynamic pricing strategies, load scheduling, and microgrid formation. Research indicates that these technologies can significantly improve energy efficiency and reduce carbon emissions. Specifically, by applying quantum optimization algorithms, researchers have demonstrated exponential classical optimizer runtime scaling even for small problem instances, suggesting that variational quantum algorithms like QAOA and hybrid quantum annealing solvers may provide more favorable runtime scaling while obtaining similar solution quality. These initial results suggest that quantum computing could be a key enabling technology in the future energy transition [2].

E. *Application in Spectrum Sensing and Management*

Quantum computing also holds a revolutionary potential for applications in spectrum sensing, especially integrated with classical reinforcement learning. One of the primary advantages of quantum computing is its efficiency in processing large volumes of data and processing complex computations. In terms of spectrum sensing, this means quantum algorithms can analyze the electromagnetic spectrum at quicker speeds with better precision, identify unoccupied channels, and optimize channel usage, thus enhancing communication efficiency and reducing interference of data.

The improvement of reinforcement learning in this field enables systems to learn optimal spectrum allocation strategies through interactions with the environment. Specifically, Quantum Deep Q Networks (QDQN) using VQC enhance the policy selection and decision-making processes in learning by approximating the deep Q-value function with quantum circuits, enhancing decision-making with less memory consumption. This method not only reduces mere parameters in the model but also use the use of quantum information encoding schemes to achieve superior performance compared to traditional neural networks.

III. Quantum Computing Affects and Future Directions

Quantum computing is transforming various fields by utilizing the unique principles of quantum mechanics. This section explores the significant impacts of quantum computing on communication, cybersecurity, artificial intelligence, and spectrum management. We will discuss both the current advancements and the future directions, highlighting the transformative potential of quantum technologies in these areas.

A. *Affects and Future Directions in Communications*

Quantum computing method, especially application of QKD, intrinsically has advantages on security which utilizes uncertainty and entanglement to ensure the privacy in channel and prevent multi-user communication from eavesdropper. Additionally, quantum computer has higher computing speed compared to a classical computer, especially for complex algorithms and large datasets, where researchers are able to use this advantage to accelerate data processing in communication.

Although quantum computing has revealed potentials, many researches are in the early stage of development, which involve complex technologies and expensive experimental setups, limiting its widespread application. It is challenging to integrate the quantum communication technologies with existing communication network infrastructures. Current network architectures might need significant adjustments to fully leverage the benefits of quantum technologies.

To overcome the decay and loss of quantum information in transmission at distance, it is necessary to develop quantum repeaters and quantum storage. It is highlighted in the context of building practical quantum communication networks, which include quantum repeaters to extend the range limit of quantum transmissions without loss of information integrity [6].

We can also enhance the quantum algorithms for efficiency by using quantum walk computing. The need for enhanced quantum algorithms specifically optimized for applications like data encryption and secure communications. This involves developing new algorithms that leverage quantum properties, such as entanglement, to perform tasks that are impractical with classical computers [7].

B. *Affects and Future Directions in Cybersecurity*

As there is an increase in connected devices, the growth of cyberattacks, and the adoption of cloud-based technologies have accelerated the need for advanced security measures like Zero Trust (ZT), which can be enhanced by quantum computing. Some have discussed the integration of AI with Zero Trust Architecture (ZTA) [8] and cybersecurity in terms of chaos theory. Both chaos theory and quantum computing offer advanced methods for analyzing and securing complex systems. For quantum-safe cryptography, quantum-resistant algorithms are essential for protecting data against future quantum attacks. Technologies such as QKD can enhance the trust and security of cryptographic keys. Quantum computing enables the enforcement of more granular and scalable security policies. It plays an important role for the dynamic and context-aware access controls required by ZTA. Quantum computing can enhance visibility with massive parallel processing power, and be able to response to potential threats.

Quantum computing principles, such as superposition and entanglement, make quantum systems inherently more secure against certain types of attacks. For instance, the nature of quantum information makes it extremely difficult to intercept or tamper with data without detection, thereby enhancing the overall security posture of systems that leverage quantum technologies. Despite quantum computing introducing new challenges to existing cybersecurity frameworks, it also provides robust solutions for enhancing security. Quantum algorithms like Grover's can search unsorted databases quadratically faster than classical algorithms [9], benefiting fields such as big data analytics, machine learning, and artificial intelligence by enabling quicker insights and solutions.

Adopting these advanced technologies and redefining foundational security principles will be crucial in addressing the evolving threat landscape in a future dominated by quantum computing. By incorporating quantum-resistant cryptography, scalable policy enforcement, enhanced visibility, and advanced automation, organizations can fortify their ZTA and significantly boost their overall cybersecurity defenses, also employing quantum sensors to detect subtle environmental changes for real-time threat identification [9].

The primary impact of quantum computing on cryptographic algorithms lies in its ability to break traditional encryption methods. Shor's algorithm, a quantum algorithm, can efficiently solve the integer factorization problem and the discrete logarithm problem. These problems form the basis of widely used cryptographic schemes such as Rivest-Shamir-Adleman (RSA) algorithm and Elliptic Curve Cryptography (ECC). As a result, these classical cryptographic methods become vulnerable to quantum attacks, threatening the security of data encrypted using these techniques [10].

The theoretical foundations suggested several potential future applications in the field of quantum computing security. The study of Gröbner bases and their complexity can be directly applied to develop and analyze cryptographic protocols that are resistant to quantum attacks [10]. These protocols will be crucial in securing communications and data in a post-quantum world. The use of affine semi-regular polynomial sequences in constructing public-key cryptographic methods, which can utilize the complexity of Gröbner basis computations to provide enhanced security against both classical and quantum attack.

The concept of cryptographic semi-regular sequences, which are easier to compute yet maintain high security, can be further explored to design robust cryptographic systems. These systems would balance computational efficiency with security, making them practical for real-world applications [10].

C. *Affects and Future Directions in AI/ML*

Quantum deep reinforcement learning (QDRL) represents a significant advancement in the integration of quantum computing with AI. By employing VQCs, researchers have optimized the traditional DQN architecture, achieving reductions in memory requirements and the number of model parameters. This approach boost policy selection and decision-making processes in reinforcement learning, effectively approximating deep Q-value functions through target networks and experience replay mechanisms [4].

In the realm of QML, the primary goal is to enhance security. QML systems exhibit unique vulnerabilities to adversarial attacks, necessitating the development of robust defense mechanisms. Techniques such as adversarial training and quantum differential privacy have been proposed to strengthen the security and reliability of QML systems in practical applications [5].

Hybrid quantum-classical machine learning architectures are another innovative application, particularly effective in processing real-time data from space-based sensors. For instance, integrating quantum neural networks with data from the Lightning Imaging Sensor (LIS) aboard the International Space Station (ISS) demonstrates the feasibility and potential of quantum-enhanced models for complex data processing tasks. This hybrid approach significantly improves data processing speed and accuracy, highlighting the practical benefits of quantum computing in real-world scenarios [11].

In the rapidly evolving field of computer vision, quantum computing offers solutions that significantly enhance efficiency. Quantum algorithms excel in solving tasks such as multi-object tracking (MOT) and transformation estimation. By reformulating these tasks into quadratic unconstrained binary optimization (QUBO) problems and utilizing quantum annealers, researchers have achieved more efficient solutions than those offered by classical methods. These studies underscore quantum computing's potential to handle computationally intensive tasks in computer vision [12].

Quantum computing in AI and ML faces significant challenges. Current noisy intermediate-scale quantum (NISQ) devices are hindered by high error rates and the absence of quantum error correction, making it difficult to effectively simulate complex deep learning models. Developing efficient quantum algorithms that do not excessively consume resources remains a formidable challenge [4] [12].

The application of quantum computing in AI and ML promises substantial reductions in computational time and energy consumption, offering capabilities beyond those of classical supercomputers. For example, quantum-enhanced models used in space data processing have demonstrated significant improvements in speed and accuracy [11].

Furthermore, quantum algorithms provide substantial speedups for certain types of problems. Grover's algorithm, for instance, can search unsorted databases quadratically faster than any classical algorithm, making it highly effective for applications requiring extensive data search and analysis. This acceleration is particularly beneficial in fields like big data analytics, machine learning, and artificial intelligence, where large datasets and complex computations are common [10].

In summary, quantum computing applications in AI and ML show transformative potential in modern research but addressing the technical challenges associated with the is crucial for widespread adoption. By advancing hybrid architectures and developing efficient quantum algorithms, quantum computing is poised to revolutionize artificial intelligence and machine learning.

D. *Affects and Future Directions in Spectrum Sensing and Management*

To enhance spectrum sensing and management, quantum computing is introduced in Cognitive Self-Organizing Networks (CSONs) [1]. This method allows for dynamic and efficient utilization of underused frequency bands without causing interference to primary users.

The incorporation of quantum computing into spectrum management is feasible by encoding spectrum occupancy information into quantum states, where cognitive radios can detect available spectrum opportunities with improved precision in highly dynamic and congested environments. This leads to more effective spectrum utilization and increased network throughput.

However, integrating quantum computing into spectrum sensing and management lies under several challenges. The complexity of quantum technologies and the need for specialized hardware which hinder widespread implementation. Additionally, quantum-based systems must ensure that they do not introduce new vulnerabilities into the network security framework. Facing these challenges, the framework incorporates quantum-resistant cryptographic technique to protect sensitive information and prevent unauthorized access, thus enhancing the security and reliability of spectrum sharing operations. Current research is also focused on developing robust quantum sensors and algorithms that can operate effectively under practical network conditions.

Future research directions should include further exploration of the applications of quantum computing across different industries, particularly in energy management and smart grids. The potential of quantum optimization technologies in energy grid optimization, dynamic pricing, and microgrid formation needs further investigation to fully exploit the advantages of quantum computing. Researchers are working on developing efficient quantum algorithms that can operate effectively without excessively consuming resources, demonstrating significant advantages in practical applications [2].

In the perspective of spectrum management, the potential of quantum computing is vast. As the quantum technologies advanced, as mentioned above, future research aims the scalability of these systems into larger network deployments. Integrating machine learning with quantum computing has the potential to redefine spectrum sensing algorithms, allowing adaptability, more effectively to adopt various network conditions.

IV. Conclusion

Quantum computing is set to bring transformative advancements across multiple domains. In communications, technologies like QKD are expected to revolutionize secure data transfer. The future of quantum communication will focus on integrating these advancements with existing network infrastructures and developing quantum repeaters to enhance long-distance communication without data loss. These improvements promise a more secure and efficient communication landscape.

In the realm of cybersecurity, quantum computing presents both significant opportunities and challenges. While it offers advanced security solutions such as QKD, it also introduces risks to existing cryptographic systems through quantum algorithms that can break traditional encryption methods. Future efforts will emphasize the development of quantum-resistant algorithms and the incorporation of quantum principles to create more robust and secure systems against evolving cyber threats.

For AI and ML, quantum computing holds great potential by enabling faster and more efficient processing of complex computations. Future research will likely focus on hybrid quantum-classical architectures to enhance computational efficiency and accuracy. Addressing current challenges, such as high error rates in quantum devices, will be essential to fully realize the potential of quantum computing in AI/ML applications.

Quantum computing also offers innovative solutions for spectrum sensing and management by improving the precision and efficiency of detecting available channels and optimizing spectrum utilization. Future developments will need to tackle the complexity of integrating quantum technologies with existing systems and ensure that these innovations do not introduce new security vulnerabilities. As quantum technologies mature, their application in spectrum management promises more effective and adaptive network operations.

Quantum computing is expected to revolutionize various fields by providing unprecedented capabilities that enhance security, optimize data processing, and improve system efficiencies. While significant challenges remain, ongoing research and interdisciplinary collaboration will be crucial in overcoming these obstacles. Successfully addressing these challenges will reveal all of the potentials from quantum technologies, leading to a future that is more secure, efficient, and intelligent.

Acknowledgements

This work was supported by the University of Massachusetts Dartmouth's Marine and Undersea Technology (MUST) Research Program funded by the Office of Naval Research (ONR) under Grant No. N00014-20-1-2170.

References

[1] C. S and S. J. Thangaraj, "Quantum-assisted spectrum sharing in cognitive self-organizing networks," in *2023 4th International Conference on Smart Electronics and Communication (ICOSEC)*, 2023, pp. 579–584.

[2] J. Blenninger, D. Bucher, and G. Cortiana, "Quantum optimization for the future energy grid summary and quantum utility prospects by jonas blenninger," 2022, pp. 29–38.

[3] D. Dequal, L. T. Vidarte, V. R. Rodriguez, and G. Vallone, "Feasibility of satellite-to-ground continuous-variable quantum key distribution," 2023.

[4] S. Lokes, C. S. J. Mahenthar, S. P. Kumaran, P. Sathyaprakash, and V. Jayakumar, "Implementation of quantum deep reinforcement learning using variational quantum circuits," in *2022 International Conference on Trends in Quantum Computing and Emerging Business Technologies (TQCEBT)*, 2022, pp. 1–4.

[5] N. Franco, A. Sakhnenko, and L. Stolpmann, "Predominant aspects on security for quantum machine learning literature review," 2024, pp. 1–8.

[6] G. T. Sridhar, A. P, and N. Tabassum, "A review on quantum communication and computing," in *2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, 2023, pp. 1592–1596.

[7] X. Qiang, S. Ma, and H. Song, "Review on quantum walk computing theory, implementation, and application," 2024.

[8] A. I. Weinberg and K. Cohen, "Zero trust implementation in the emerging technologies era - survey," 2024.

[9] M. Njorbuenwu, B. Swar, and P. Zavarsky, "A survey on the impacts of quantum computers on information security," 2019.

[10] M. Kudo, "Onhilbert-poincar´e series of affine semi-regular polynomial sequences and related gr¨obner bases," 2024.

[11] S. Fadli and B. S. Rawal, "Hybrid quantum-classical machine learning for near real-time space to ground communication of iss lightning imaging sensor data," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, 2023, pp. 0114–0122.

[12] H. T. Larasati, T.-T.-H. Le, and H. Kim, "Trends of quantum computing applications to computer vision," in *2022 International Conference on Platform Technology and Service (PlatCon)*, 2022, pp. 7–12.

[13] G. Arun and V. Mishra, "A review on quantum computing and communication," in *2014 2nd International Conference on Emerging Technology Trends in Electronics, Communication and Networking*, 2014, pp. 1–5.

[14] A. A. Yavuz, S. E. Nouma, T. Hoang, D. Earl, and S. Packard, "Distributed cyber-infrastructures and artificial intelligence in hybrid post-quantum era," in *2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, 2022, pp. 29–38.

[15] D. Barral, F. J. Cardama, and G. Diaz, "Review of distributed quantum computing. from single qpu to high performance quantum computing," 2024.

[16] M. J. Hossain Faruk, S. Tahora, M. Tasnim, H. Shahriar, and N. Sakib, "A review of quantum cybersecurity: Threats, risks and opportunities," in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, 2022, pp. 1–8.

[17] Y. J. Gambo, T. Shinde, K. Rasch, H. Liebelt, and R. Li, "Simulation of the quantum key distribution algorithm using the intel quantum sdk," in *2023 13th International Conference on Advanced Computer Information Technologies (ACIT)*, 2023, pp. 492–495.

[18] M. Alvarado and L. Gayler, "A survey on post-quantum cryptography state-of-the-art and challenges," 2023, pp. 1–16.

[19] D. Rosch-Grace and J. Straub, "Analysis of the necessity of quantum computing capacity development for national defense and homeland security," 2021.

[20] S. F. Ahmad, M. Y. Ferjani, and M. Y. Ferjani, "Enhancing security in the industrial iot sector using quantum computing," 2021.

[21] J. Moazzam, R. Pawar, and M. D. Khare, "Evolution and advancement of quantum computing in the era of networking and cryptography," 2023.

[22] S. Ambika, V. Balaji, R. Rajasekaran, P.N.Periyasamy, and N. Kamal, "Explore the impact of quantum computing to enhance cryptographic protocols and network security measures," 2024.

[23] P. Mukherjee and R. K. Barik, "Fog-qkd:towards secure geospatial data sharing mechanism in geospatial fog computing system based on quantum key distribution," 2022.

[24] T. M. Fernández-Caramés, "From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things," 2020.

[25] I.Anantraj, B. Umarani, C. Karpagavalli, C. Usharani, and S. J. Lakshmi, "Quantum computing's double-edged sword unravelling the vulnerabilities in quantum key distribution for enhanced network security," 2023.