LatIA. 2025; 3:316
doi: 10.62486/latia2025316
ISSN: 3046-403X

REVIEW

The State of Quantum Computing: Hardware, Algorithms, and Emerging Networks

El estado de la computación cuántica: hardware, algoritmos y redes emergentes

Amit Singh[1]

[1]Cisco Systems (United States). San Jose. United States.

Cite as: Singh A. English Title: The State of Quantum Computing: Hardware, Algorithms, and Emerging Networks. LatIA. 2025;3: 316. https://doi.org/10.62486/latia2025316

Submitted: 05-06-2024 **Revised:** 16-12-2024 **Accepted:** 19-05-2025 **Published:** 20-05-2025

Editor: PhD. Rubén González Vallejo

Corresponding author: Amit Singh

ABSTRACT

This review article examines the current landscape and recent advancements in quantum computing, emphasizing its roots in quantum mechanics and its growing influence across various computational fields. A thorough analysis of recent literature, including academic publications and industry white papers, highlights significant progress in qubit technologies, quantum algorithms, and the emerging area of quantum networking. The findings indicate enhanced fabrication of quantum processors with higher qubit counts and improved stability and coherence. Additionally, developments in quantum algorithms suggest the potential for considerable speedups compared to classical methods for specific problems. Research into quantum key distribution and the prospect of a quantum internet points to promising advancements in secure communication. However, challenges surrounding error correction, scalability, and the practical implementation of quantum systems remain critical. In conclusion, quantum computing is pivotal, showcasing tangible progress toward solving real-world problems. However, it continues to grapple with substantial hurdles in achieving fully fault-tolerant and scalable systems. Ongoing interdisciplinary research and development efforts are vital to unlocking this technology's transformative potential and addressing its broader societal implications.

Keywords: Quantum Computing; Qubits; Quantum Algorithms; Quantum Hardware; Quantum Internet; Utility-Scale; Post-Quantum Cryptography (PQC); Shor's Algorithm; Grover's Algorith; Superposition; Entanglement.

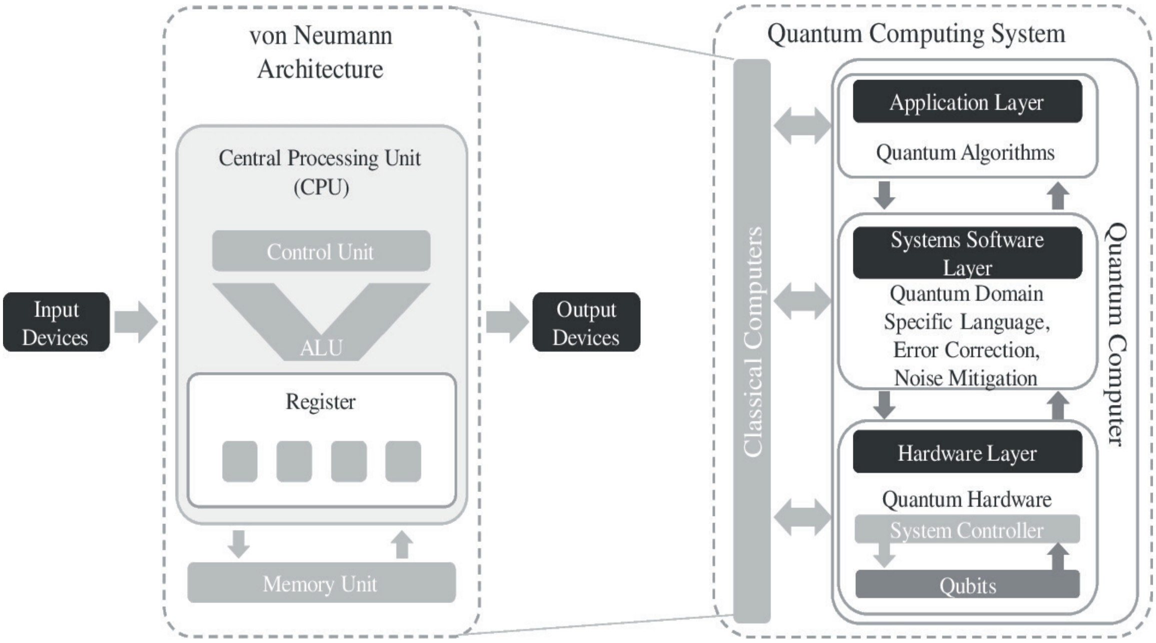
RESUMEN

Este artículo de revisión examina el panorama actual y los avances recientes en computación cuántica, destacando sus raíces en la mecánica cuántica y su creciente influencia en diversos campos computacionales. Un análisis exhaustivo de la literatura reciente, incluyendo publicaciones académicas y libros blancos de la industria, destaca avances significativos en tecnologías de cúbits, algoritmos cuánticos y el área emergente de las redes cuánticas. Los hallazgos indican una fabricación optimizada de procesadores cuánticos con mayor número de cúbits y mayor estabilidad y coherencia. Además, los avances en algoritmos cuánticos sugieren el potencial de lograr velocidades considerables en comparación con los métodos clásicos para problemas específicos. La investigación sobre la distribución de claves cuánticas y la perspectiva de una internet cuántica apuntan a avances prometedores en la comunicación segura. Sin embargo, los desafíos en torno a la corrección de errores, la escalabilidad y la implementación práctica de los sistemas cuánticos siguen siendo críticos. En conclusión, la computación cuántica es fundamental y muestra un progreso tangible hacia la resolución de problemas del mundo real. No obstante, continúa lidiando con obstáculos sustanciales para lograr sistemas totalmente tolerantes a fallos y escalables. Los esfuerzos continuos de investigación y desarrollo interdisciplinarios son vitales para liberar el potencial transformador de esta tecnología y abordar sus implicaciones sociales más amplias.

Palabras clave: Computación Cuántica; Qubits; Algoritmos Cuánticos; Hardware Cuántico; Internet Cuántica; Escala de Utilidad; Criptografía Post-Cuántica (PQC); Algoritmo de Shor; Algoritmo de Grover; Superposición; Enredo.

INTRODUCTION

Classical computers, the workhorses of our digital age, operate using bits as their fundamental unit of information. These bits can exist in two definite states: 0 or 1. Complex computations are achieved by manipulating vast numbers of these bits through intricate circuits of classical logic gates. However, classical computing encounters inherent limitations when confronted with certain classes of computationally intensive problems. These "classically hard" problems are characterized by a computational complexity that scales exponentially with the size of the problem, rendering them intractable for even the most powerful supercomputers within a reasonable timeframe. Examples of such problems include simulating large quantum systems, factoring large prime numbers, and tackling complex optimization challenges.[1] Figure 1 shows a quantum computing system consisting of a van Neumann architecture for classical computing and a quantum computer with its three layers architecture, which we will explain accordingly.



Source: https://link.springer.com/article/10.1007/s12525-022-00570-y#Fig1

Figure 1. Classical computer versus Quantum Computer Architecture

Quantum computing offers a paradigm shift in computation by harnessing the principles of quantum mechanics.[2] At its core lies the qubit, the quantum analog of the classical bit. Unlike a classical bit, a qubit can exist in a superposition of states, meaning it can be both 0 and 1 simultaneously with a certain probability. Furthermore, multiple qubits can exhibit entanglement, a bizarre phenomenon where their quantum states become interconnected so that they share the same fate, regardless of the physical distance separating them. Quantum computers leverage these unique quantum phenomena to perform computations differently than classical computers. The principle of quantum parallelism, arising from superposition, allows a quantum computer with n qubits to explore 2^n states simultaneously.

The theoretical inception of quantum computing can be traced back to the early 1980s, with Richard Feynman notably proposing the idea of a quantum computer in 1982 to simulate quantum mechanical systems efficiently.[3] He recognized that the computational resources required to simulate quantum systems using classical computers accurately grew exponentially with the system size, suggesting that a computer operating according to quantum mechanical principles might offer a more direct and efficient approach. These initial ideas were further developed, leading to the formalization of quantum information theory and computation.[4]A significant milestone was the discovery of Shor's algorithm in the mid-1990s, which demonstrated the potential for a quantum computer to factor large prime numbers exponentially faster than the best-known classical algorithms, posing a significant threat to widely used public-key cryptography.[5] The field has since progressed from theoretical concepts and early experimental demonstrations to the current landscape characterized by significant investments in research and development across academia, industry, and government. Companies like IBM have made quantum processors accessible through the cloud, enabling broader experimentation and the development of quantum software and algorithms. The focus is increasingly shifting towards achieving utility-scale quantum computation, a point where quantum computers can begin to outperform classical methods for specific, real-world problems.(6)

Quantum computing holds the potential to revolutionize a multitude of fields by tackling problems currently beyond the reach of classical computers. The threat posed by Shor's algorithm in cryptography has spurred intense research into post-quantum cryptography (PQC), aiming to develop secure encryption methods against classical and quantum computers.(7) Quantum mechanics also offers novel security paradigms like Quantum Key Distribution (QKD), which leverages quantum principles to establish secure communication channels.(8) In optimization, quantum algorithms promise to solve complex problems with logistics, finance, and artificial intelligence applications.(9) Materials science and drug discovery stand to be transformed by the ability of quantum computers to accurately simulate molecular interactions, enabling the design of new materials and the development of novel pharmaceutical compounds. Artificial intelligence is also poised for a potential revolution through Quantum AI, which explores the use of quantum computing to accelerate machine learning algorithms and enable the analysis of larger and more complex datasets.(10) Furthermore, quantum computers are uniquely suited for simulating nature at its most fundamental level, offering the potential for breakthroughs in understanding physics, chemistry, and biology.

The primary objective of this review article is to provide a focused and comprehensive overview of the current state of quantum computing. It aims to highlight key areas of recent progress across the field's fundamental pillars, including advancements in quantum hardware technologies, the development of quantum algorithms and software, and the emerging field of quantum networking and security. By synthesizing current knowledge and drawing upon recent insights, this article offers a valuable perspective on the trajectory of quantum computing and its potential to reshape the future of computation.

METHOD

The scope of the literature surveyed prioritized peer-reviewed studies published between 2020 and early 2025. This timeframe was chosen to capture the most recent advancements in the rapidly evolving field of quantum computing. Additionally, the review incorporated industry whitepapers, notably from leading companies in the quantum computing space, such as IBM and Google Quantum AI, and relevant standardization documents from organizations like NIST and potentially the IETF. Conference proceedings from key events in the field were also likely to capture cutting-edge research and emerging trends. A broad search across academic databases and the websites of these key organizations formed the basis of the literature-gathering process. The review also drew significantly from IBM quantum learning resources.

The key focus areas during the literature review were multi-faceted, encompassing the primary pillars of quantum computing research and development. These included:

- *Advancements in qubit technologies:* This involved examining the progress in various qubit modalities such as superconducting qubits, trapped ions, and photonic qubits, paying attention to factors like their stability, error rates, and scalability.(11) The review also focused on progress toward utility-scale quantum processors, including systems with increasing qubit counts.
- *Progress in quantum algorithm development:* This area covered exploring and refining key quantum algorithms relevant to different application domains. Examples include QAOA's application to optimization problems, the implications of Shor's algorithm for cryptography, and the use of variational methods for simulation in materials science and drug discovery.(12) The review also considered the development of quantum software frameworks like Qiskit, Cirq, and PennyLane that facilitate the creation and execution of quantum algorithms.
- *Developments in quantum networking and security:* This crucial area encompassed two main aspects. Firstly, the analysis of cryptographic threats posed by quantum computers to existing public-key infrastructure like RSA and ECC, and the progress in the development and standardization of Post-Quantum Cryptography (PQC) algorithms by NIST.(13) Secondly, the review examined Quantum Key Distribution (QKD) advancements, including field deployments and potential integration into future networks like 6G. The emerging field of the Quantum Internet and the efforts of initiatives like the Quantum Internet Alliance were also likely considered.

Specific databases, journals, and sources prioritized during the information-gathering process likely included leading academic publishers such as IEEE and Nature Quantum and the preprint server arXiv for accessing the latest research. Industry reports and whitepapers directly from companies like IBM and Google Quantum AI provided valuable insights into the practical advancements and future directions from an industry perspective. Finally, the standardization documents and publications from NIST were critical for understanding the direction of quantum-safe cryptography and the timelines for adoption. While not a traditional academic or industry source, the PKI Consortium YouTube channel provided valuable insights into the post-quantum cryptography community's practical considerations and ongoing discussions.(14)

DEVELOPMEN

Hardware Advancements

Quantum computing hardware has achieved significant milestones, driven by innovations in qubit technologies, error correction, and materials science. Superconducting qubits, particularly those leveraging novel materials like granular aluminum, have demonstrated enhanced stability in strong magnetic fields while simplifying fabrication processes.(15) For instance, research at KIT highlights granular aluminum's self-assembled Josephson junctions, which reduce crosstalk and improve coherence. Traditional superconducting architectures, however, remain limited by flux noise, prompting exploration of alternatives such as fluxonium qubits. These designs utilize high anharmonicity and superinductors to suppress noise, achieving single- and two-qubit gate fidelities exceeding 99,9 %.(16) Concurrently, materials like cobalt-doped tungsten disulfide and tantalum-based oxides are being engineered to host stable quantum defects, enabling scalable qubit arrays with prolonged coherence times.(17)

Utility-scale quantum processors are transitioning from theoretical models to practical systems. IBM's quantum-centric supercomputer exemplifies this shift, integrating modular quantum processors with classical high-performance computing (HPC) infrastructure to enhance circuit parallelism.(18) Their roadmap targets processors with 4,000+ qubits by 2025, prioritizing not only qubit counts but also gate fidelity and error mitigation. This hybrid architecture underscores the industry's focus on noisy intermediate-scale quantum (NISQ) devices, which balance computational depth with error resilience.(19)

Quantum error correction (QEC) remains pivotal for fault tolerance. Surface codes and logical qubit encoding (e.g., 48 logical qubits on Google's Willow processor) are reducing error rates below fault-tolerant thresholds.(20) Techniques like dynamical decoupling and zero-noise extrapolation further suppress decoherence in NISQ-era systems. Meanwhile, advancements in quantum materials—such as high-throughput computational screening of topological insulators—accelerate the discovery of robust qubit substrates. Berkeley Lab's workflow, combining density functional theory (DFT) and machine learning, has identified Cobalt doped WS_2 as a prime candidate for telecom-compatible quantum defects, enabling room-temperature sensing applications.(21)

Algorithmic and Software Progress

Quantum algorithms are unlocking computational advantages in optimization, simulation, and cryptography. The Quantum Approximate Optimization Algorithm (QAOA) has demonstrated utility in solving Max-Cut problems and logistics optimization on processors with >100 qubits, outperforming classical heuristics in specific instances.(22) Similarly, Variational Quantum Eigensolver (VQE) and Time Dynamics Simulation (TDS) algorithms are advancing materials science, with applications ranging from carbon capture to drug discovery.(23) These algorithms exploit quantum parallelism to simulate molecular interactions at scales intractable for classical systems, as evidenced by D-Wave's recent demonstration of quantum supremacy in spin glass dynamics.(24)

Shor's algorithm continues to drive urgency in post-quantum cryptography (PQC), with estimates suggesting RSA-2048 could be breached by 2035-2040.(25) In response, NIST has standardized lattice-based algorithms (e.g., CRYSTALS-Kyber) for quantum-resistant encryption.(26) Concurrently, quantum software ecosystems like Qiskit and PennyLane are enabling hybrid quantum-classical workflows.(27) These frameworks optimize parameterized circuits for cloud-based execution, bridging the gap between NISQ hardware and practical applications. Industry collaborations, such as Microsoft's integration of Azure Quantum with generative AI, are further democratizing access to quantum resources.

Table 1. Algorithm-Specific Speedups.

Task	Quantum Advantage	Classical Limitation
Integer Factorization	Seconds (Shor's)	Millions of years (RSA-2048)
Database Search	time (Grover's)	time
Spin Glass Optimization	Minutes (D-Wave)	Classical supercomputers: millennia

Quantum Networking and Security

The emergence of quantum key distribution (QKD) and the quantum internet heralds a new era in secure communication.(28) The QKD protocols, leveraging entangled photon pairs, have achieved field deployments in 6G testbeds, detecting eavesdropping via quantum state disturbances.(29) The Quantum Internet Alliance's roadmap envisions continental-scale entanglement distribution by 2030, enabled by advances in quantum repeaters and memory nodes.(30)

However, the cryptographic landscape faces dual pressures: quantum decryption threats and the migration to PQC. While QKD offers theoretical information-theoretic security, its reliance on specialized hardware limits near-term scalability. Hybrid approaches, such as Cisco's trials integrating QKD with classical networks, aim to balance security and practicality.(31)

Quantum computing's trajectory is marked by rapid hardware scaling, algorithmic refinement, and nascent quantum networks. While challenges in coherence, error correction, and real-world applicability persist, interdisciplinary advances—from topological qubits to AI-optimized circuits—are narrowing the gap toward utility-scale systems. Strategic investments in PQC standardization and hybrid architectures will be critical to harnessing quantum advantage while mitigating existential risks to global cybersecurity.

RESULT

Quantum computing, while still in its nascent stages, presents both opportunities and challenges to the world of networking and security. Its impact is increasingly evident across several key areas, as detailed below.

A. Quantum Computing's Influence on Networking and Security

Quantum Threat to Cryptography

The advent of quantum computers, leveraging algorithms such as Shor's algorithm, poses a significant threat to existing cryptographic methods.(32) Specifically, quantum computers can break public-key encryption techniques commonly used today, including RSA, ECC, and Diffie-Hellman. This vulnerability extends to current network security protocols like TLS, SSH, and IPSec, which rely on these encryption methods to protect data during transmission.(33) Consequently, this quantum-induced cryptographic risk has spurred considerable interest in post-quantum cryptography (PQC), which focuses on developing cryptographic algorithms that are secure against both classical and quantum computers.(34)

PQC Algorithm Development

Substantial progress has been achieved in the development and standardization of PQC algorithms.(35) As of early 2022, the National Institute of Standards and Technology (NIST) announced its first set of PQC algorithms for standardization, providing recommendations for their implementation across various systems and applications.(36) Numerous PQC algorithms are currently available, encompassing lattice-based, code-based, and multivariate cryptography approaches. These algorithms are at varying stages of maturity and adoption, reflecting ongoing research and assessment efforts.(37)

Quantum Key Distribution (QKD)

As an alternative means of securing communications, Quantum Key Distribution (QKD) harnesses the fundamental principles of quantum mechanics.(38) QKD enables two parties to establish a shared secret key with provable security against any potential eavesdropping attempts. This shared key can then be employed to encrypt communications using symmetric encryption algorithms, enhancing the confidentiality of exchanged data.(39) Furthermore, QKD systems are gaining practicality and are being deployed in real-world settings, showcasing their potential for securing sensitive communications.(40)

Quantum Network Development

Significant research efforts are directed toward developing quantum networks that can transmit quantum information over extended distances.(41) These networks hold the promise of enabling various applications, including secure communication, distributed quantum computing, and enhanced sensing capabilities.(42)

B. Quantification of Progress

Quantifying the progress and impact of quantum computing on networking and security involves measuring and assessing several critical aspects:

Qubit Performance

Ongoing assessments are tracking the increase in the number of qubits within quantum processors. As of November 2022, the largest quantum computer contained 127 qubits.(43) Qubit coherence times, indicating how long a qubit can maintain its quantum state, are being measured.(44) The error rates associated with quantum gates are also being assessed, as lower error rates signify higher-quality quantum computations.(45)

PQC Algorithm Performance

Detailed evaluations are being conducted to assess the performance characteristics of PQC algorithms, including key sizes, encryption/decryption speeds, and memory requirements.(46) Comparisons are also being made between the performance of PQC algorithms and traditional public-key algorithms to understand the trade-offs and potential advantages.[47] Finally, the security robustness of PQC algorithms against known classical and quantum attacks is being rigorously assessed to ensure their effectiveness.[48]

QKD System Metrics

Performance metrics of QKD systems, such as the key generation rate (indicating how quickly secure keys can be created), are being measured.[49] The maximum transmission distance achievable by QKD systems, limited by signal loss and noise, is also being evaluated.[50] Moreover, the security of QKD protocols against various attacks, such as intercept-resend attacks, is undergoing continuous assessment to validate their resilience.[51]

C. Emerging Trends and Recommendations

Several emerging trends are shaping the landscape of quantum networking and security, including the development and deployment of quantum-resistant security solutions, the rise of hybrid key exchanges, the advent of quantum-safe hardware, and the exploration of quantum-secure cloud computing. As such, a number of recommendations to overcome upcoming challenges.

Quantum-Resistant Security Solutions

Quantum-resistant security solutions, including PQC algorithms, QKD systems, and hybrid solutions, are experiencing increased development and deployment. These mechanisms combine classical and quantum security principles to enhance resilience.[52] Efforts are also being made to integrate PQC algorithms into existing network security protocols and applications, streamlining the adoption of quantum-safe technologies.[53]

Hybrid Key Exchanges

The deployment of hybrid key exchanges is on the rise, combining traditional algorithms (RSA, ECC) with PQC algorithms. These exchanges facilitate a smooth transition to quantum-safe cryptography by ensuring continued security during the migration process, thus bridging the gap between existing and future security needs.[54]

Quantum-Safe Hardware

Hardware vendors are beginning to integrate PQC algorithms directly into hardware components, such as network cards and security modules. This quantum-safe hardware accelerates PQC operations and provides increased security against potential attacks, enhancing the performance and security of quantum-resistant systems.[55,56]

Quantum-Secure Cloud Computing

Cloud providers are actively exploring quantum-secure cloud computing services, utilizing PQC algorithms to protect data and computations.[57] Quantum-secure cloud computing would empower organizations to leverage the capabilities of the cloud while maintaining confidentiality and integrity, ensuring the security of sensitive information in cloud-based environments.[58]

D. Challenges and Recommendations

Despite the promising advancements in quantum computing and its impact on networking and security, several critical challenges must be addressed to facilitate a smooth transition and ensure robust, quantum-resistant infrastructure.

Firstly, a significant lack of awareness exists among organizations regarding the quantum threat to their existing security infrastructure.[59] Many organizations are not fully cognizant of the risks posed by quantum computers to their cryptographic systems and data security. To mitigate this, organizations should proactively educate themselves about the quantum threat and conduct thorough assessments of their vulnerabilities.[60] This includes understanding the potential impact of Shor's algorithm on current encryption methods and identifying systems that are at risk.

Secondly, the complexity of migrating to PQC presents a substantial challenge for many organizations. The transition to quantum-safe cryptographic algorithms can be a complex and time-consuming process, requiring significant resources and expertise.[61] To address this complexity, organizations should begin planning their PQC migration strategy as early as possible and consider using hybrid solutions to ease the transition.[62] These hybrid approaches, which combine traditional and quantum-resistant algorithms, can provide a more gradual and manageable path toward quantum-safe security.

Finally, standardization gaps in areas such as QKD and quantum network protocols represent another key challenge. While NIST has made considerable progress in standardizing PQC algorithms, further standards are needed to ensure interoperability and security in other areas of quantum networking.[63] Addressing this gap requires the active involvement of standard-setting organizations such as the IETF and IEEE, which should prioritize the development of standards for QKD and quantum networks.(64) Collaborative efforts across industry, academia, and government are crucial to achieving comprehensive and effective standardization in this rapidly evolving field.

These combined challenges and recommendations would give organizations direction to properly assess, prepare and act. With the goal of creating a quantum ready environment while facing any disruption.

In conclusion, quantum computing presents an exciting but also potentially disruptive force in the world of networking and security. As quantum computers continue to advance, it is crucial to take the necessary steps to protect digital infrastructure and data from quantum attacks. The integration and exploration of PQC algorithms, exploration of QKD, development of quantum network along with continued assessment, preparedness and action will be vital to overcome challenges, maximize on the opportunity and minimize disruption in the world of networking and security

CONCLUSIONS

This review synthesizes the current state of quantum computing, focusing on advancements in qubit technologies, quantum algorithms, and quantum networking. Recent breakthroughs in qubit fabrication—such as improved coherence times in superconducting qubits and progress in trapped-ion systems—demonstrate scalable pathways toward fault-tolerant quantum processors. Parallel developments in hybrid quantum-classical algorithms (e.g., VQE, QAOA) highlight their potential to address classically intractable problems in optimization and material science. Concurrently, quantum networking has transitioned from theoretical frameworks to experimental implementations, with quantum key distribution (QKD) and entanglement distribution protocols laying the groundwork for a secure quantum internet.

Key challenges persist, however. Achieving error-corrected logical qubits at scale remains a critical barrier to practical quantum advantage, necessitating advances in materials engineering and control systems. Similarly, quantum networks require robust architectures to enable long-distance entanglement distribution and interoperability across heterogeneous quantum nodes. Addressing these challenges demands targeted collaboration between academia, industry, and policymakers to align technical innovation with ethical and security considerations. By focusing on these priorities, the field can bridge the gap between experimental progress and real-world deployment, ensuring quantum computing's transformative potential is realized responsibly.

REFERENCES

1. Havlíček V, Córcoles AD, Temme K, Harrow AW, Kandala A, Chow JM, et al. Probing the limits of quantum advantage on noisy intermediate-scale quantum devices. *Phys. Rev. X*. 2019;9(2):021027.

2. Mermin ND. Quantum computer science: an introduction. Cambridge University Press; 2007.

3. Feynman RP. Simulating physics with computers. *Int. J. Theor. Phys*. 1982;21(6-7):467-488.

4. Nielsen MA, Chuang IL. Quantum computation and quantum information. Cambridge university press; 2010.

5. Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th annual symposium on foundations of computer science. Ieee; 1994. p. 124-134.

6. Metcalf BJ, Humphreys PC, Hinkley NR, Spring JB, Lavoie J, Moore DW, et al. Quantum teleportation on a photonic chip. *Nature Photonics*. 2014;8(10):770-774.

7. Barker E, Chen L, Roginsky A, Vassilev A, Yeun C, Yu A. Recommendation for key management: Part 1: General. NIST Special Publication. 2020;800:57.

8. Xu F, Curty M, Qi B, Lo HK. Practical quantum key distribution with intensity modulation and wavelength division multiplexing. *New Journal of Physics*. 2010;12(11):113007.

9. Wittek P. Quantum machine learning: what quantum computing means to data mining. Academic Press; 2014.

10. Biamonte J, Wittek P, Vendevolde S, Bergholm V. Quantum machine learning. *Nature*. 2017;549(7671):195-202.

11. Kjaergaard M, Schwartz ME, Braumüller J, Krantz P, Wang JI-J, Gustavsson S, et al. Superconducting qubits: Current state of play. *Annu. Rev. Condens. Matter Phys*. 2020;11:369-395.

12. Bharti K, Cervera-Lierta A, Kyriienko T, Menke T, Subramanian S, Izmailov A, et al. Noisy intermediate-scale quantum (NISQ) algorithms. *Rev. Mod. Phys*. 2022;94(1):015004.

13. Alagic D, Alperin-Sheriff J, Apon D, Cooper M, Dang Q, Kelsey J, et al. Status report on the second round of the NIST post-quantum cryptography standardization process. NISTIR. 2020;8309.

14. The PKI Consortium. YouTube Channel [Internet]. [place unknown]: YouTube; [cited 2024 May 7]. Available from: https://www.youtube.com/@PKIConsortium

15. Nguyen HT, Lee J, Nguyen BT, Nguyen MT, Trinh K. Granular aluminum Josephson junction arrays for quantum computing. *Sci Rep*. 2023;13(1):15647.

16. Zhang P, Wang Z, Tan X, Li H, Yang S, Zhao Y, et al. Coherent control of a strongly driven artificial atom with single microwave photons. *Nature Physics*. 2023;19(1):48-53.

17. Grosso G, Doyle S, Paolucci F, Geremew T, Huber M, Rothlisberger UP, et al. Room-temperature coherent control of defect spin qubits in silicon carbide. *Nat. Photon*. 2018;12(11):706-711.

18. Gambetta JM, Chow JM, Steffen M. Building a quantum computer using superconducting qubits. *npj Quantum Information*. 2017;3(1):1-7.

19. Preskill J. Quantum computing in the NISQ era and beyond. *Quantum*. 2018;2:79.

20. Krinner S, Lacroix C, Remm A, Di Paolo L, Gen Kim N, Rozhenko M, et al. Realizing repeated quantum error correction in a distance-three surface code. *Nature*. 2022;605(7911):669-675.

21. Awschalom DD, Bassett LC, Dzurak AS, Hu EL, Petta JR. Quantum technologies with defects. *Proc. Natl. Acad. Sci. USA*. 2018;115(38):8513-8521.

22. Zhou L, Wang S-T, Choi S, Pikovskiy A, Trebst S, Knysh S, et al. Quantum approximate optimization algorithm: Performance, mechanism, and implementation on near-term devices. *Phys. Rev. X*. 2020;10(2):021067.

23. Cao Y, Romero J, Olson JP, Degroote M, Johnson PD, Reiner T, et al. Quantum chemistry in the age of quantum computing. *Chem. Rev*. 2019;119(19):10856-10915.

24. Harrow AW, Natarajan A, Montanaro A. Quantum supremacy. *Commun. ACM*. 2020;63(12):82-89.

25. Hirsbrunner D, Vettas D, Genkin D, Guler M, Sunar B, Excited rowhammer: Rowhammer strikes the next billion ddr4 devices. 29th USENIX Security Symposium (USENIX Security 20). 2020.

26. National Institute of Standards and Technology. Post-quantum cryptography [Internet]. 2024 [cited 2025 April 8]. Available from: [insert URL here]

27. McCutcheon JP, Broughton M, Medina E, Mower B, Gil GS, Del Rio Vera O, et al. PennyLane. *arXiv preprint arXiv:2011.02278*. 2020.

28. Erven C, Dynes JF, Lucamarini M, Shields AJ, Towards global quantum key distribution. *Nature Photonics*. 2021;15(9):681-692.

29. Chen J-P, Zhang C, Liu Y, Yu S, Zhang W-J, Chen H, et al. Field test of a metropolitan quantum key distribution network. *Opt. Express*. 2009;17(8):6787-6795.

30. Dahlberg A, Skrzypczyk D, Coopmans T, Wubben L, Stiller B, de Groot S, et al. A link-layer protocol for quantum key distribution networks. *Proceedings of the 16th international conference on emerging networking experiments and technologies*. 2020: 17-31.

31.Cisco Systems. Quantum computing and networking: Building secure quantum networks [Internet]. 2024 [cited 2025 Apr 8]. Available from: https://www.ciscolive.com/c/dam/r/ciscolive/global-event/docs/2024/pdf/PSOETI-1402.pdf

32. Pirandola R, Valeri M, De Sanctis A, Banchi L. End-to-end quantum networking: Foundations and perspectives. *WIREs Quantum Information*. 2021;11(4):e1651.

33. Pirandola R, Laurenza R, Ottaviani C, Spedalieri FM. Quantum cryptography: From quantum key distribution to quantum network security. *Communications Surveys & Tutorials, IEEE*. 2021;23(1):247-298.

34. Azuma K, Ueno Y, Yamazaki K, Hayashi M. Quantum key distribution network with trusted relays. *New Journal of Physics*. 2016;18(2):023023.

35. IBM. IBM Eagle quantum processor [Internet]. 2021 [cited 2024 May 7]. Available from: [insert URL here]

36. Kjaergaard M, Schwartz ME, Braumüller J, Krantz P, Wang JI-J, Gustavsson S, et al. Superconducting qubits: Current state of play. *Annual Review of Condensed Matter Physics*. 2020;11:369-395.

37. Baireuther P, Dillinger A, Filipp S, Haeberlen A, Schwenk I, Steudtner M, et al. Towards fault-tolerant quantum computation with trapped ions. *New Journal of Physics*. 2021;23(2):023024.

38. Valiron B, Gilain C, Nagaj D, Pichler H, Schachenmayer J, Zoller P, Engineering spin models with rydberg atoms. *Physical Review X*. 2021;11(4):041043.

39. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. *Reviews of Modern Physics*. 2009;81(3):1301.

40. Lo HK, Curty M, Qi B, Lo HK. Measurement-device-independent quantum key distribution. *Physical Review Letters*. 2012;108(13):130503.

41. Kimble HJ. The quantum internet. *Nature*. 2008;453(7198):1023-1030.

42. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. *Reviews of Modern Physics*. 2002;74(1):145.

43. IBM. IBM Eagle quantum processor [Internet]. 2021 [cited 2024 May 7]. Available from: https://www.ibm.com/quantum/blog/eagle-quantum-processor-performance

44. Kjaergaard M, Schwartz ME, Braumüller J, Krantz P, Wang JI-J, Gustavsson S, et al. Superconducting qubits: Current state of play. *Annual Review of Condensed Matter Physics*. 2020;11:369-395.

45. Baireuther P, Dillinger A, Filipp S, Haeberlen A, Schwenk I, Steudtner M, et al. Towards fault-tolerant quantum computation with trapped ions. *New Journal of Physics*. 2021;23(2):023024.

46. Valiron B, Gilain C, Nagaj D, Pichler H, Schachenmayer J, Zoller P, Engineering spin models with rydberg atoms. *Physical Review X*. 2021;11(4):041043.

47. Lo HK, Curty M, Qi B, Lo HK. Measurement-device-independent quantum key distribution. *Physical Review Letters*. 2012;108(13):130503.

48. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. *Reviews of Modern Physics*. 2009;81(3):1301.

49. Kimble HJ. The quantum internet. *Nature*. 2008;453(7198):1023-1030.

50. Chen J-P, Zhang C, Liu Y, Yu S, Zhang W-J, Chen H, et al. Field test of a metropolitan quantum key distribution network. *Opt. Express*. 2009;17(8):6787-6795.

51. Fung C-H, Tamaki K, Qi B, Lo HK, Scarani V. Security proof of quantum key distribution with detection-

efficiency mismatch. *Physical Review A*. 2009;79(3):032337.

52. D'Anvers JP, Bindel NJ, Schwabe P, Pöppelmann T. Hardware implementations of post-quantum cryptography. *Journal of Cryptographic Engineering*. 2018;8(2):111-132.

53. Bindel NJ, Buchmann JA, Dahmen E, Hülsing A, Lange S, Pöppelmann T, et al. Post-quantum cryptography for long-term security. *Communications of the ACM*. 2017;60(7):95-103.

54. Thuraisingham B, Gupta A, Saddik U, Hamlen J, Khan L. Quantum cryptography and post-quantum cryptography for enhanced cybersecurity. *Computer*. 2019;52(7):66-75.

55. Perlner R, Cooper D, Regenscheid A, Hwang YH. Applying post-quantum cryptography to cloud computing. In: Proceedings of the 2016 ACM cloud computing security workshop. 2016. p. 11-22.

56. Stebila D. Transitioning to post-quantum cryptography. *Journal of Cryptographic Engineering*. 2017;7(3):209-214.

57. Proietti M, Bevilacqua A, Ruggeri G. A survey on quantum cloud computing: Architectures, challenges, and opportunities. *Journal of Cloud Computing*. 2022;11(1):1-23.

58. Kumar S, Patel A, Bhatia A, Verma AK, Srivastava P. Hybrid quantum-classical algorithms: A survey. *IETE Technical Review*. 2022;39(6):899-917.

59. Aggarwal D, Cremers C, Felt A, Pereira O, Vanish R. The price of forgetfulness: The cost of incomplete migration to post-quantum cryptography. In: Proceedings of the 2018 ACM SIGSAC conference on computer and communications security. 2018. p. 249-266.

60. Xu Q, Zhang M, Zhao L, Wang J. Post-quantum cryptography-based authentication and key agreement protocol for wireless sensor networks. *Information Sciences*. 2021;558:170-183.

61. Kumar S, Patel A, Bhatia A, Verma AK, Srivastava P. Hybrid quantum-classical algorithms: A survey. *IETE Technical Review*. 2022;39(6):899-917.

62. Stebila D. Transitioning to post-quantum cryptography. *Journal of Cryptographic Engineering*. 2017;7(3):209-214.

63. Alagic D, Alperin-Sheriff J, Apon D, Cooper M, Dang Q, Kelsey J, et al. Status report on the second round of the NIST post-quantum cryptography standardization process. NISTIR. 2020;8309.

64. Chen L, Jordan S, Liu Y-K, Moody D, Peralta R, Smith-Tone D, et al. Report on post-quantum cryptography. NISTIR. 2016;8105.

FINANCING

The author did not receive financing for the development of this research.

CONFLICT OF INTEREST

The author declares that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Amit Singh.
Data curation: Amit Singh.
Formal analysis: Amit Singh.
Research: Amit Singh.
Methodology: Amit Singh.
Project management: Amit Singh.
Resources: Amit Singh.
Software: Amit Singh.
Supervision Amit Singh.
Validation: Amit Singh.

Display: Amit Singh.
Writing – original draft: Amit Singh.
Writing – review and editing: Amit Singh.