Orissa Journal of Physics
ISSN 0974-8202

Vol. 33, No.1
February 2026
pp. 68-83

Quantum Computing Algorithms

RAKESH MOHAN PUJAHARI[1, *] and M. C. ADHIKARY[2]

[1]Lloyd Institute of Engineering and Technology, Greater Noida, Uttar Pradesh, India
[2]Dept. of Physics, Fakir Mohan University, Balasore, Odisha, India
[*]Corresponding author, E-mail: rpujahari@gmail.com

Abstract. This essay explores the state of quantum computing today and its latest developments, highlighting its foundations in quantum physics and its expanding impact in a number of computer domains. Significant advancements in qubit technologies, quantum algorithms, and the developing field of quantum networking are highlighted via a careful examination of current literature, including scholarly articles and business white papers. The results show better stability and coherence as well as improved fabrication of quantum processors with greater qubit counts. Furthermore, advances in quantum algorithms point to the possibility of significant speedups over classical approaches for some applications. Promising developments in secure communication are indicated by research into quantum key distribution and the possibility of a quantum internet. However, there are still significant issues with error correction, scalability, and the real-world application of quantum systems. To sum up, quantum computing is essential, demonstrating observable advancements in the resolution of practical issues. However, it still faces significant challenges in developing truly scalable and fault-tolerant systems. To fully realize the revolutionary potential of this technology and address its wider societal ramifications, ongoing interdisciplinary research and development activities are essential.

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

1. INTRODUCTION

Bits are the basic unit of information used by classical computers, the workhorses of our digital age. There are two distinct states in which these bits can exist: 0 and 1. Large numbers of these bits are manipulated using complex circuits of classical logic gates to perform complex computations. However, when faced with some kinds of computationally demanding problems, classical computing faces intrinsic limits. Even the most powerful supercomputers are unable to solve these "classically hard" issues in a reasonable amount of time due to their computational complexity, which grows exponentially with problem size. These

issues involve factoring big prime numbers, simulating large quantum systems, and solving challenging optimization problems. (1) Figure 1 depicts a quantum computing system made up of a three-layered quantum computer and a van Neumann architecture for classical computing, which we shall explain in turn.

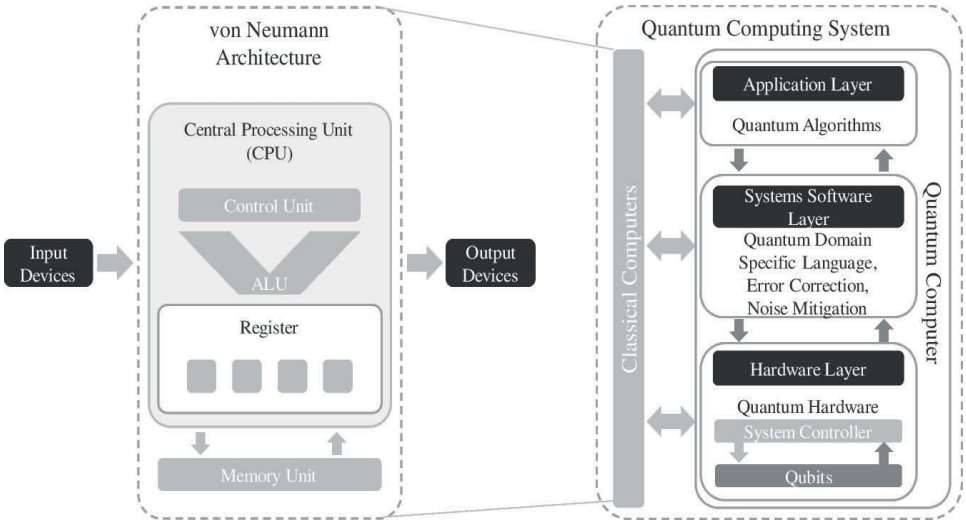

Figure 1. Classical computer versus Quantum Computer Architecture

By utilizing the concepts of quantum mechanics, quantum computing provides a paradigm change in computation.(2) The qubit, the quantum counterpart of the classical bit, is its central component. A qubit, in contrast to a traditional bit, can exist in a superposition of states, which means that it has a specific probability of being both 0 and 1 at the same time. Moreover, entanglement—a strange phenomena in which the quantum states of several qubits become interconnected so that they share the same fate regardless of the physical distance between them—can occur. These special quantum events are used by quantum computers to carry out computations in a different way than traditional computers. A quantum computer with n qubits can simultaneously explore 2^n states thanks to the principle of quantum parallelism, which results from superposition.

Richard Feynman famously proposed the concept of a quantum computer in 1982 to effectively replicate quantum mechanical systems, marking the theoretical beginning of quantum computing in the early 1980s.(3) He noticed that the processing resources needed to accurately replicate quantum systems using classical computers increased exponentially with the size of the system, indicating that a computer functioning in accordance with quantum mechanical

principles would provide a more straightforward and effective solution. Quantum information theory and computation were formalized as a result of the development of these basic concepts.(4)

The discovery of Shor's algorithm in the mid-1990s was a major turning point since it showed that a quantum computer could factor big prime numbers exponentially faster than the most well-known classical algorithms, posing a serious threat to commonly used public-key cryptography.(5) Since then, the area has advanced from theoretical ideas and early practical demonstrations to the present state of affairs, which is marked by large investments in government, business, and academic research and development. In order to facilitate more extensive experimentation and the creation of quantum software and algorithms, companies such as IBM have made quantum processors available via the cloud. The goal of attaining utility-scale quantum computation—a stage at which quantum computers can start to outperform classical approaches for particular, practical issues—is becoming more and more important.(6) By solving issues that classical computers are now unable to handle, quantum computing has the potential to completely transform a wide range of industries. Intense research into post-quantum cryptography (PQC), which aims to create safe encryption techniques against both classical and quantum computers, has been sparked by the threat posed by Shor's algorithm in cryptography.(7) New security paradigms like as Quantum Key Distribution (QKD), which uses quantum principles to create secure communication channels, are also provided by quantum mechanics.(8) Quantum algorithms in optimization have the potential to resolve challenging issues with applications in artificial intelligence, finance, and logistics.(9)

The ability of quantum computers to precisely simulate molecular interactions has the potential to revolutionize materials science and drug discovery by facilitating the creation of innovative medicinal compounds and new materials. Quantum AI, which investigates the use of quantum computing to speed up machine learning algorithms and enable the study of bigger and more complicated datasets, is another potential revolution in artificial intelligence.Ten Additionally, quantum computers have the potential to advance our knowledge of physics, chemistry, and biology by mimicking nature at its most basic level.

This review article's main goal is to give a thorough and targeted summary of the state of quantum computing today. It seeks to highlight significant recent developments in the core pillars of the subject, such as improvements in quantum

hardware technologies, the creation of quantum software and algorithms, and the burgeoning field of quantum networking and security. This article provides a useful viewpoint on the development of quantum computing and its potential to transform computation in the future by combining existing knowledge with new discoveries.

2. Principle of the design method

Peer-reviewed research released between 2020 and early 2025 were given priority in the survey's scope. This period of time was selected to encompass the latest developments in the quickly developing field of quantum computing. The review also included industry whitepapers, particularly from top quantum computing companies like IBM and Google Quantum AI, as well as pertinent standardization publications from NIST and maybe the IETF. Cutting-edge research and new trends were also likely to be captured in conference papers from significant events in the area. The procedure of acquiring material was based on a thorough search of scholarly databases and the websites of these important organizations. IBM quantum learning resources were also heavily referenced in the report.

The fundamental pillars of quantum computing are:

2.1 Advancements in qubit technologies:

This required analyzing the development of different qubit modalities, including photonic qubits, trapped ions, and superconducting qubits, while keeping an eye on things like their scalability, error rates, and stability. (11) The development of utility-scale quantum processors, including systems with growing qubit counts, was also a focus of the assessment.

2.2 Progress in quantum algorithm development:

In this field, important quantum algorithms pertinent to several application domains were investigated and improved. Examples include the use of variational approaches for modeling in materials research and drug discovery, the use of QAOA to optimization problems, and the implications of Shor's algorithm for cryptography. (12) The development of quantum software frameworks that make it easier to create and run quantum algorithms, such as Qiskit, Cirq, and PennyLane, was also taken into consideration.

2.3 Developments in quantum networking and security

There were two primary components to this important area. First, the creation and standardization of Post-Quantum Cryptography (PQC) algorithms by NIST, as well as the examination of the cryptographic risks that quantum computers represent to current public-key infrastructure such as RSA and ECC.(13) Second, the assessment looked at developments in Quantum Key Distribution (QKD),

such as field implementations and possible incorporation into upcoming networks like 6G. The work of organizations like the Quantum Internet Alliance and the developing field of the Quantum Internet were probably also taken into account.

Leading academic publishers like IEEE and Nature Quantum, as well as the preprint service arXiv enabling access to the most recent research, were probably among the specific databases, journals, and sources that were given priority during the information-gathering process. Direct industry reports and whitepapers from businesses like IBM and Google Quantum AI offered insightful information about the useful developments and potential future paths from an industry standpoint. Lastly, the NIST papers and standardization documents were essential for comprehending the trajectory of quantum-safe cryptography and the adoption deadlines. The PKI Consortium YouTube channel offered insightful information about the practical issues and current debates in the post-quantum cryptography world, despite not being a conventional academic or industry source.(14)

3. Development

3.1 Hardware Advancements

Thanks to advancements in materials science, error correction, and qubit technologies, quantum computing hardware has reached important milestones. Superconducting qubits have shown improved stability in strong magnetic fields while streamlining production procedures, especially when utilizing cutting-edge materials like granular aluminium.(15).For example, KIT research emphasizes the self-assembled Josephson junctions in granular aluminium, which enhance coherence and decrease crosstalk. However, flux noise continues to limit traditional superconducting topologies, leading to the investigation of alternatives like fluxonium qubits. These devices achieve single- and two-qubit gate fidelities surpassing 99.9% by suppressing noise with high anharmonicity and super inductors.(16) At the same time, stable quantum defects are being built into materials such as tantalum-based oxides and cobalt-doped tungsten disulfide to enable scalable qubit arrays with extended coherence periods.(17) From theoretical models to real-world systems, utility-scale quantum processors are evolving. This change is best shown by IBM's quantum-centric supercomputer, which combines modular quantum processors with traditional high-performance computing (HPC) infrastructure to improve circuit parallelism.(18)

By 2026, their roadmap aims for processors with more than 4,000 qubits, giving gate fidelity and error mitigation equal weight with qubit counts. The industry's emphasis on noisy intermediate-scale quantum (NISQ) devices, which strike a compromise between computational depth and error resilience, is shown by this hybrid architecture. (19) For fault tolerance, quantum error correction (QEC) is still essential. Error rates are falling below fault-tolerant levels thanks to surface codes and logical qubit encoding (such as the 48 logical qubits on Google's Willow processor).(20) Decoherence in NISQ-era systems is further suppressed by methods such as zero-noise extrapolation and dynamical decoupling. Meanwhile, the search for reliable qubit substrates is accelerated by developments in quantum materials, such as high-throughput computational screening of topological insulators. Cobalt doped WS2 has been recognized by Berkeley Lab's workflow, which combines density functional theory (DFT) and machine learning, as a top candidate for telecom-compatible quantum

Cobalt doped WS2 is a prime candidate for telecom-compatible quantum defects, enabling room-temperature sensing applications, according to Berkeley Lab's process, which combines density functional theory (DFT) and machine learning.(21)

3.2 Algorithmic and Software Progress

Computational advantages in cryptography, simulation, and optimization are being unlocked by quantum algorithms. On processors with more than 100 qubits, the Quantum Approximate Optimization Algorithm (QAOA) has shown useful in solving Max-Cut issues and logistics optimization, sometimes surpassing traditional methods.(22) In a similar vein, materials science is being advanced via Variational Quantum Eigen solver (VQE) and Time Dynamics Simulation (TDS) algorithms, which have applications ranging from drug discovery to carbon capture.(23) As demonstrated by D-Wave's recent demonstration of quantum supremacy in spin glass dynamics, these algorithms take advantage of quantum parallelism to model molecular interactions at sizes intractable for classical systems.(24)

Post-quantum cryptography (PQC) is still under pressure due to Shor's algorithm; estimations indicate that RSA-2048 may be compromised by 2035–2040. For quantum-resistant encryption, NIST has developed standardized lattice-based algorithms, such as CRYSTALS-Kyber.(26) At the same time, hybrid quantum-classical operations are made possible by quantum software ecosystems such as Qi skit and PennyLane.(27) These frameworks bridge the gap

between NISQ hardware and real-world applications by optimizing parameterized circuits for cloud-based execution. Access to quantum resources is becoming more accessible because to industry partnerships like Microsoft's integration of Azure Quantum with generative AI.

3.3 Quantum Networking and Security

A new age in secure communication is being ushered in by the development of quantum key distribution (QKD) and the quantum internet.(28) By using entangled photon pairs to detect eavesdropping through quantum state disruptions, the QKD algorithms have successfully deployed in 6G testbeds.(29) According to the Quantum Internet Alliance's plan, advancements in quantum repeaters and memory nodes would enable continental-scale entanglement dissemination by 2030.(30)

However, there are two pressures on the cryptographic landscape: the shift to PQC and the possibility of quantum decryption. Although QKD provides information-theoretic security, its near-term scalability is limited by its dependence on specialized technology. The goal of hybrid systems, like Cisco's experiments combining QKD with traditional networks, is to strike a compromise between security and usefulness. (31)
Rapid hardware growth, algorithmic improvement, and emerging quantum networks are characteristics of the trajectory of quantum computing. Interdisciplinary developments—from topological qubits to AI-optimized circuits—are closing the gap toward utility-scale systems, despite ongoing difficulties with coherence, error correction, and practical applicability. Harnessing quantum advantage while reducing existential dangers to global cybersecurity would need strategic investments in PQC standardization and hybrid architectures.

4. RESULT

Although it is still in its early phases, quantum computing offers networking and security both potential and challenges. As explained below, its influence is becoming more noticeable in a number of important areas.

A. Quantum Computing’s Influence on Networking and Security

Quantum Threat to Cryptography: Existing encryption techniques are seriously threatened by the development of quantum computers, which use algorithms like Shor's algorithm.(32) In particular, public-key encryption methods like RSA, ECC, and Diffie-Hellman that are widely used today can be cracked by quantum

computers. Current network security protocols like TLS, SSH, and IPSec, which depend on these encryption techniques to safeguard data during transmission, are also vulnerable.(33) As a result, post-quantum cryptography (PQC), which focuses on creating cryptographic algorithms that are safe against both classical and quantum computers, has attracted a lot of attention due to this quantum-induced cryptographic danger.(34)

PQC Algorithm Development: The research and standardization of PQC algorithms have advanced significantly.(35) The first set of PQC algorithms for standardization was released by the National Institute of Standards and Technology (NIST) in early 2022, along with suggestions for their applicability in different systems and applications. (36) There are currently many PQC algorithms available, including multivariate, code-based, and lattice-based cryptography techniques. As a result of continuous research and evaluation activities, these algorithms are in different stages of adoption and maturity. (37)

Quantum Key Distribution (QKD): Quantum Key Distribution (QKD) uses the basic ideas of quantum physics as an alternative method of communication security.(38) Two parties can create a shared secret key with provable security against any possible eavesdropping efforts thanks to QKD. The confidentiality of transmitted data can then be improved by utilizing this shared key to encrypt communications using symmetric encryption methods. (39) Additionally, QKD systems are becoming more practical and being used in actual situations, demonstrating its promise for protecting private communications.(40)

Quantum Network Development: The development of quantum networks capable of transmitting quantum information over long distances is the focus of significant scientific efforts.(41) A number of applications, such as distributed quantum computing, secure communication, and improved sensing capabilities, could be made possible by these networks.(42)

B. Quantification of Progress

Measuring and evaluating a number of crucial factors is necessary to quantify the development and effects of quantum computing on networking and security:

Qubit Performance: The rise in the quantity of qubits in quantum processors is being monitored by ongoing evaluations. The largest quantum computer had 127 qubits as of November 2022.(43) Measurements are being made of qubit coherence times, which show how long a qubit can sustain its quantum state.(44)

Since lower error rates indicate higher-quality quantum calculations, the error rates related to quantum gates are also being evaluated.(45)

PQC Algorithm Performance: The performance aspects of PQC algorithms, such as key sizes, encryption/decryption speeds, and memory needs, are being thoroughly evaluated.(46) To comprehend the trade-offs and possible benefits, comparisons between the performance of PQC algorithms and conventional public-key algorithms are also being made.(47) Lastly, to guarantee the efficacy of PQC algorithms, its security resilience against known conventional and quantum assaults is being thoroughly evaluated.(48)

QKD System Metrics: QKD system performance parameters are being measured, such as the key generation rate, which shows how fast secure keys can be generated.(49) Additionally, the maximum transmission distance that QKD systems may achieve, constrained by noise and signal loss, is being assessed.(50) Additionally, ongoing evaluations are being conducted to confirm the resilience of QKD protocols against a variety of assaults, including intercept-resend attacks.(51)

A. Emerging Trends and Recommendations

The development and implementation of quantum-resistant security solutions, the emergence of hybrid key exchanges, the introduction of quantum-safe hardware, and the investigation of quantum-secure cloud computing are some of the new developments that are reshaping the field of quantum networking and security. Thus, several suggestions for overcoming future obstacles.

Quantum-Resistant Security Solutions: PQC algorithms, QKD systems, and hybrid solutions are examples of quantum-resistant security solutions that are being developed and implemented more often. To improve robustness, these approaches incorporate both classical and quantum security concepts.(52) In order to expedite the deployment of quantum-safe technology, efforts are also being undertaken to incorporate PQC algorithms into current network security protocols and applications.(53)

Hybrid Key Exchanges: Hybrid key exchanges, which combine conventional methods (RSA, ECC) with PQC algorithms, are becoming more widely used. By guaranteeing ongoing security throughout the migration process, these exchanges help to bridge the gap between current and future security requirements and enable a seamless transition to quantum-safe cryptography.(54)

Quantum-Safe Hardware: Hardware manufacturers are starting to include PQC algorithms straight into hardware parts like security modules and network cards. The performance and security of quantum-resistant systems are improved by using quantum-safe hardware, which speeds up PQC processes and increases security against prospective attacks.(55, 56)

Quantum-Secure Cloud Computing: In order to safeguard data and calculations, cloud providers are actively investigating quantum-secure cloud computing services using PQC algorithms.(57) By guaranteeing the security of sensitive data in cloud-based environments, quantum-secure cloud computing would enable businesses to take advantage of the cloud's advantages while upholding confidentiality and integrity.(58)

A. Challenges and Recommendations

Notwithstanding the encouraging developments in quantum computing and its implications for networking and security, a number of crucial issues need to be resolved to enable a seamless transition and guarantee reliable, quantum-resistant infrastructure.

First of all, enterprises are mostly unaware of the quantum danger to their current security infrastructure. (59) Many businesses are unaware of the dangers quantum computers pose to their data security and cryptography systems. Organizations should proactively educate themselves about the quantum danger and thoroughly evaluate their vulnerabilities in order to mitigate this.(60) This entails figuring out which systems are vulnerable and comprehending how Shor's algorithm can affect existing encryption techniques.

Second, many firms find it extremely difficult to transition to PQC due to its complexity. It can be difficult and time-consuming to switch to quantum-safe cryptographic methods, requiring a lot of resources and knowledge.(61) Organizations should start developing their PQC migration strategy as soon as feasible in order to handle this complexity, and they should think about utilizing hybrid solutions to make the shift easier.(62) These hybrid strategies can offer a more progressive and controllable route to quantum-safe security by combining conventional and quantum-resistant algorithms. Lastly, another major issue is the lack of standardization in fields like quantum network protocols and QKD. Even though NIST has made significant strides in defining PQC algorithms, more standards are required to guarantee security and interoperability in other quantum networking domains.(63)

Together, these difficulties and suggestions would provide businesses with guidance on how to appropriately evaluate, plan, and respond. with the intention of establishing a quantum-ready ecosystem in the face of any interruption. In summary, quantum computing is a fascinating but possibly disruptive force in the networking and security industries. It is critical to take the required precautions to safeguard digital infrastructure and data from quantum assaults as quantum computers continue to develop. To overcome obstacles, seize opportunities, and reduce disruption in the networking and security industry, it will be essential to integrate and investigate PQC algorithms, investigate QKD, construct quantum networks, and maintain ongoing assessment, readiness, and action.

CONCLUSION

With an emphasis on developments in qubit technology, quantum algorithms, and quantum networking, this overview summarizes the state of quantum computing today. Scalable routes to fault-tolerant quantum processors are shown by recent advances in qubit production, such as enhanced coherence times in superconducting qubits and advancements in trapped-ion systems. The promise of hybrid quantum-classical algorithms, such as VQE and QAOA, to solve classically unsolvable optimization and material science issues is demonstrated by parallel breakthroughs in these algorithms. At the same time, quantum key distribution (QKD) and entanglement distribution protocols have laid the foundation for a secure quantum internet, and quantum networking has moved from theoretical frameworks to experimental implementations.

FUTURE WORK

However, major obstacles still exist. Developments in materials engineering and control systems are required to achieve error-corrected logical qubits at scale, which continues to be a crucial obstacle to practical quantum advantage. In a similar vein, robust architectures are necessary for quantum networks to provide interoperability across diverse quantum nodes and long-distance entanglement distribution. In order to address these issues, politicians, business, and academia must work together specifically to match technological progress with security and ethical concerns. By concentrating on these tasks, the field can ensure that the revolutionary potential of quantum computing is responsibly fulfilled by bridging the gap between experimental advancement and practical implementation.

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 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.
11. 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.
12. 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.
13. The PKI Consortium. YouTube Channel [Internet]. [place unknown]: YouTube; [cited 2024 May 7]. Available from: https://www.youtube.com/@PKIConsortium

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

15. 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.

16. 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.

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

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

19. 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.

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

21. 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.

22. 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.

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

24. 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.

25. National Institute of Standards and Technology. Post-quantum cryptography [Internet]. 2024 [cited 2025 April 8].

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

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

28. 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.

29. 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 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

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

31. 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.

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

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

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

35. 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.

36. 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.

37. 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.

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

39. Kimble HJ. The quantum internet. *Nature*. 2008;453(7198):1023-1030. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. *Reviews of Modern Physics*. 2002;74(1):145.

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

41. 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.

42. 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.

43. 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.

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

45. 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.

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

47. 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.

48. 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.

49. quantum cryptography. *Journal of Cryptographic Engineering*. 2018;8(2):111-132.

50. 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.

51. 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.Perlner R, Cooper D, Regenscheid A, Hwang YH. Applying post-quantum cryptography to cloud computing.

52. In: Proceedings of the 2016 ACM cloud computing security workshop. 2016. p. 11-22.

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

54. 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.

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

56. 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.

57. 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.

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. Stebila D. Transitioning to post-quantum cryptography. *Journal of Cryptographic D'Anvers JP, Bindel NJ, Schwabe P, Pöppelmann T. Hardware implementations of post-Engineering*. 2017;7(3):209-214.

60. 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.

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