iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.68369

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Quantum vs. Classical Approaches: A Comparative Study and Future Perspectives

Shailesh Palavakar[1], Vishwajit Jagtap[2], Pathan Wahid[3]
P.V.G.'s College of Science and Commerce

Abstract: ***The paper provides an exploration of quantum computing, emphasizing its potential and challenges. It begins with the fundamentals of quantum mechanics and differentiates between classical and quantum computing, focusing on concepts like qubits, superposition, and entanglement. The authors identify the existing limitations in practical quantum applications, particularly within the Noisy Intermediate-Scale Quantum (NISQ) era, where issues like noise in quantum circuits hinder scalability and reliability. The paper addresses the need for advancements in hardware, error correction techniques, and practical algorithms tailored for current technological constraints. Additionally, it discusses the implications of quantum computing on cryptography, underscoring the vulnerability of traditional cryptographic methods and the urgency for post-quantum cryptographic solutions. The methodology involves literature review, expert consultations, and bibliometric analysis to gauge global research trends in quantum computing. The paper highlights crucial research gaps, particularly in the development of scalable quantum algorithms suitable for near-future applications.***

I. INTRODUCTION

A. What is Quantum Computing?

Quantum computing is a type of computation that harnesses the principles of quantum mechanics to process information in ways that classical computers cannot. At its core, quantum computing utilizes quantum bits or qubits, which differ fundamentally from classical bits. The introduction of the paper elaborates on the fundamental principles of quantum computing and its potential to revolutionize various fields, particularly cryptography. It starts by defining key concepts such as qubits, superposition, and entanglement, drawing distinctions between classical and quantum computing methodologies. The authors discuss the technological advancements made by leading companies in the quantum computing sector, while simultaneously highlighting the existing challenges in achieving consistent and scalable quantum systems. Moreover, the introduction emphasizes the emerging threats that quantum computing poses to current cryptographic methods, especially against algorithms like RSA and Diffie-Hellman. The authors present a graph illustrating the growth of research activity in quantum computing over recent years, which visually represents the increasing global interest in the field. This graphical representation serves to underscore the urgency for advancements in post-quantum cryptography, reinforcing the call for innovative solutions to protect against vulnerabilities that quantum algorithms may exploit. The introduction effectively sets the context for the discussion on the need for robust cryptographic frameworks in the face of evolving quantum technologies.

B. Name of the Figure

Comparison between Classical Computing and Quantum Computing

Aspect	Classical Computing	Quantum Computing
Basic Unit of Data	Bit (0 or 1)	Qubit (0, 1, or both simultaneously in superposition)
Information Processing	Sequential processing	Parallel processing due to superposition maintained by qubits
Computation Power	Limited to classical algorithms with polynomial time complexity in many cases	Potential for exponential speedup over classical systems for specific problems (e.g., Shor's and Grover's algorithms)
State Representation	Distinct states (one at a time)	Multiple states represented at once due to superposition
Algorithm Complexity	Complexity classes like P, NP, and NP-complete	Quantum complexity classes like BQP, offering different efficiencies for problem-solving

Aspect	Classical Computing	Quantum Computing
Entanglement	Non-existent (bits are independent)	Qubits can be entangled, allowing their states to be interdependent, which enhances computational capability
Error Correction	Well-established methods exist	Error correction is more complex and still a developing field due to decoherence and noise in quantum systems
Practical Challenges	Maturity in technology and infrastructure	Current challenges include qubit stability, coherence times, and scaling the technology for practical use
Applications	Widely used in everyday computing, simulations, database management, etc.	Potential applications in cryptography, complex simulations, optimization problems, and artificial intelligence, yet still largely in research and development

II. METHODOLOGY

The methodology adopted in the review paper encompasses several structured phases aimed at analyzing the state of quantum computing and its impact on cryptographic systems. The following key phases outline the approach taken:

1) Literature Review: A comprehensive review of existing research and publications related to quantum computing, including foundational quantum algorithms, current technological developments, and the implications for cryptography. This helps to establish a theoretical framework and identify gaps in the current knowledge base.
2) Expert Consultations: The authors consulted with experts in the fields of quantum computing and cryptography. This provides insights into real-world applications and challenges that may not be covered in academic literature.
3) Technical Evaluations: The paper includes evaluations of quantum computing technologies, focusing on their scalability, reliability, and error correction mechanisms. This assessment involves analyzing the current state of quantum hardware and software.
4) Bibliometric Analysis: The methodology involved conducting bibliometric analysis to evaluate global engagement and trends in quantum research. This helps in quantifying research activity and identifying leading institutions or countries in quantum computing research.
5) Assessment of Challenges: The study also assesses the technical challenges associated with developing quantum computers and the feasibility of existing and potential quantum algorithms, along with their applications in cryptography.
6) Identification of Research Gaps: As part of the methodology, the authors identified significant research gaps that exist in the field, particularly regarding the development of practical quantum algorithms and post-quantum cryptography solutions.

III. GAPS AND CHALLENGES QUANTUM COMPUTING

A. *Gaps*

1) *Limited Practical Quantum Algorithms*

While foundational quantum algorithms, such as Shor's (for factoring) and Grover's (for search), have been established theoretically, there is a lack of practical algorithms designed to run on the noisy intermediate-scale quantum (NISQ) computers currently available. Most quantum algorithms require fully error-corrected quantum systems, which are not yet realized, leading to a gap between theoretical potential and practical application.

2) *Understanding of Quantum Impacts on Cryptography*

There is an insufficient understanding of how quantum algorithms fundamentally challenge existing cryptographic protocols. Although it is clear that algorithms like Shor's can break RSA and other encryption based on integer factorization, the extent of vulnerability for other symmetric and asymmetric systems under quantum attacks needs further exploration. Research is still needed to clarify the implications for cryptographic schemes not directly mentioned in seminal studies, particularly newer or less-established protocols.

3) *Lack of Scalable Solutions in Post-Quantum Cryptography*

As the development of quantum computing progresses, the need for cryptographic methods that can resist quantum attacks is becoming increasingly urgent. Despite ongoing research into post-quantum cryptography (PQC) strategies (e.g., lattice-based, code-based, multivariate polynomial), there are minimal scalable implementations suitable for widespread adoption in real-world systems. Theoretical research is advancing, but practical applications remain limited, indicating a gap in translating theory into action.

4) Material Technology Development

In the domain of quantum hardware, there is a significant gap in exploring new materials and physical implementations needed for high-performing quantum systems. While some material systems (like superconducting qubits) have shown promise, the exploration of alternative materials, such as topological qubits or photonic qubits, is still in its infancy. Developing uniform, reproducible, and stable quantum components is critical for the scalability and reliability of quantum technology.

B. Challenges

1) Scalability of Quantum Hardware

A central challenge remains the scalability of quantum computing hardware. Current quantum systems struggle with issues such as noise, short decoherence times, and error rates that increase with the number of qubits. Building a scalable quantum computer that maintains coherence over a large number of qubits is a sophisticated engineering and materials science challenge.

2) Error Mitigation and Correction

As quantum systems are scaled up, the implementation of quantum error correction becomes paramount. While methods like Shor's and Steane's error correction codes are known, their practical application is limited by resource requirements and the complexity involved in correcting errors without overwhelming the quantum processor. Developing efficient error-correcting codes that are both practical and provide a substantial fidelity boost remains a formidable challenge.

3) Integration with Classical Systems

The integration of quantum computing with existing classical computing systems (hybrid systems) introduces complexities in maintaining security and interoperability. As quantum computers begin to outpace classical systems in specific computations, building interfaces that can leverage quantum advantages without exposing potential vulnerabilities is critical. This challenge necessitates a re-evaluation of existing security protocols.

4) Continuing Research in Cryptography

The rapid pace of advancements in quantum computing necessitates an ongoing commitment to developing new cryptographic techniques. Transitioning to post-quantum cryptography poses not only theoretical challenges in design but also practical hurdles in terms of standardization, deployment, and public trust in new methods. There’s a need for comprehensive studies and frameworks that evaluate and compare the effectiveness of various PQC algorithms against quantum attacks.

5) Technical Complexity in Implementing Post-Quantum Cryptography

Many post-quantum cryptographic methods involve complex mathematical structures and algorithms that can be difficult to implement efficiently in existing systems. The technical complexity inherent in these systems presents barriers to comprehension and practical adoption among developers and organizations. Consequently, creating a robust ecosystem of libraries, tools, and resources to facilitate the development and integration of PQC methods into applications is essential.

IV. CONCLUSION

The rise of quantum computing presents both exciting opportunities and significant challenges, particularly in the field of cryptography. As quantum technologies advance, they threaten to undermine traditional cryptographic systems, necessitating urgent research and development of post-quantum cryptography that can withstand quantum attacks. Key gaps, such as the lack of practical algorithms for noisy intermediate-scale quantum (NISQ) machines and the need for scalable security solutions, highlight the need for interdisciplinary collaboration among quantum physicists, materials scientists, and cryptographers.

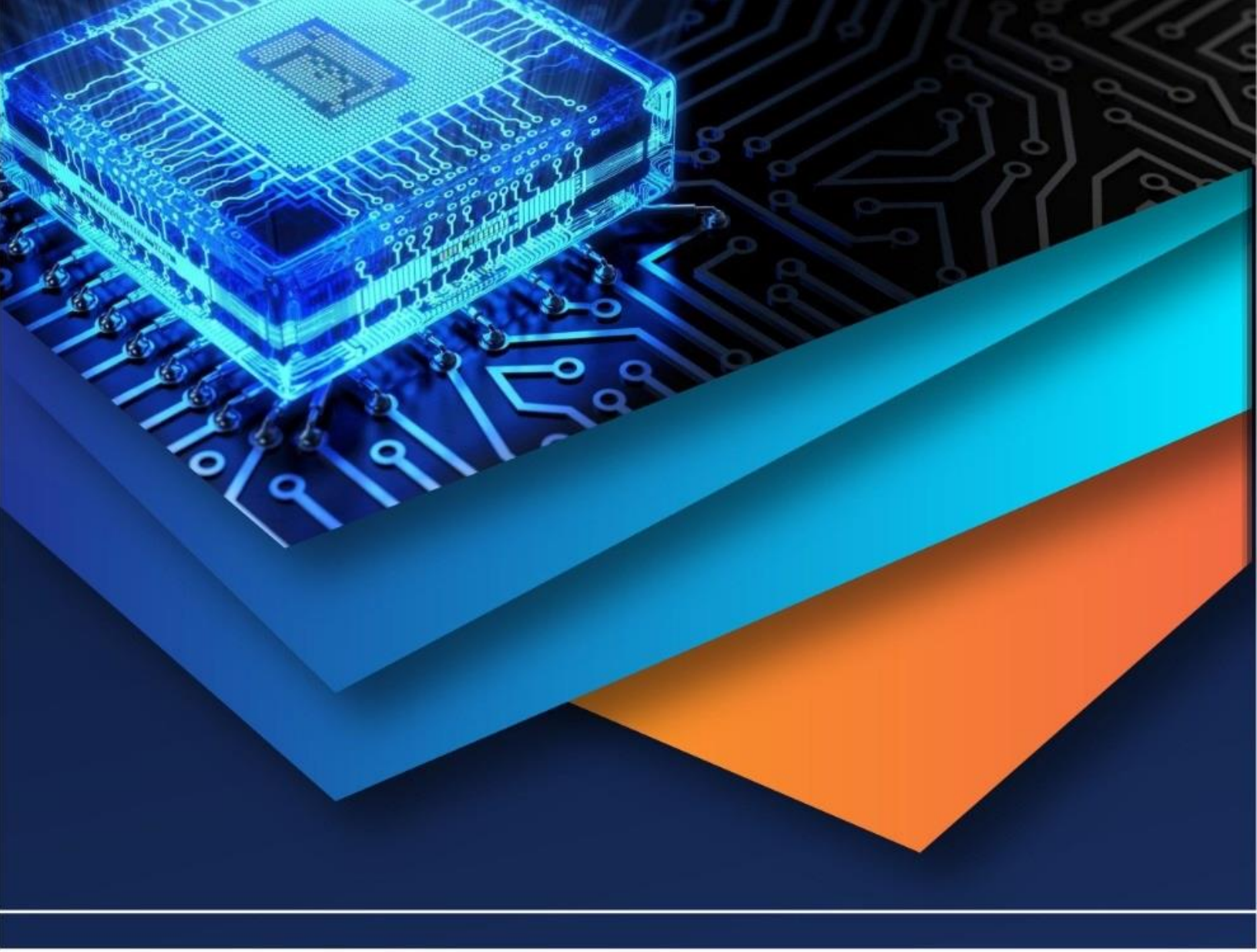
To ensure digital security in the quantum era, it is essential to proactively address these challenges and innovate robust cryptographic frameworks. By anticipating potential vulnerabilities and advancing quantum technologies, we can secure sensitive information and foster a resilient digital landscape in a rapidly evolving technological landscape.

REFERENCES

[1] Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. arXiv. https://arxiv.org/abs/1804.00200

[2] Shor, P. W. (1998). Quantum computing. MIT. https://math.mit.edu/~shor/

[3] Yati, M. (2020). Quantum cryptography. ResearchGate. https://www.researchgate.net/publication/345675328_Quantum_Cryptography
[4] State-of-the-art analysis of quantum cryptography. (2024). Frontiers in Physics. https://www.frontiersin.org/journals/physics/articles/10.3389/fphy.2024.1456491/full
[5] Quantum computing and cryptography: Analysis, risks, and recommendations. (2019). Lawrence Livermore National Laboratory. https://cgsr.llnl.gov/sites/cgsr/files/2024-08/QuantumComputingandCryptography-20190920.pdf
[6] Quantum cryptography and quantum key distribution. (n.d.). IEEE Xplore. https://ieeexplore.ieee.org/document/9726722/
[7] Quantum computing in cryptography. (2023). ResearchGate. https://www.researchgate.net/publication/377845746_Quantum_Computing_in_Cryptography
[8] The impact of quantum computing on post-quantum cryptography. (2023). SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4904933
[9] Quantum cryptography for enhanced network security. (2022). arXiv. https://arxiv.org/pdf/2306.09248
[10] Alvarado, M., Gayler, L., Seals, A., Wang, T., & Hou, T. (2023). A survey on post-quantum cryptography: State-of-the-art and challenges. arXiv. https://arxiv.org/abs/2312.10430
[11] Upadhyay, S., Roy, R., & Ghosh, S. (2023). Designing hash and encryption engines using quantum computing. arXiv. https://arxiv.org/abs/2310.17439
[12] Mamatha, G. S., Dimri, N., & Sinha, R. (2024). Post-quantum cryptography: Securing digital communication in the quantum era. arXiv. https://arxiv.org/abs/2403.11741
[13] Arute, F., Arya, K., Babbush, R., et al. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505-510. https://doi.org/10.1038/s41586-019-1666-5
[14] Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79. https://doi.org/10.22331/q-2018-08-06-79
[15] Bennett, C. H., & Wiesner, S. J. (1992). Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Physical Review Letters, 69(20), 2881–2884. https://doi.org/10.1103/PhysRevLett.69.2881
[16] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC), 212–219. https://doi.org/10.1145/237814.237866
[17] Nielsen, M. A., & Chuang, I. L. (2010). Quantum computation and quantum information. Cambridge University Press.
[18] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126. https://doi.org/10.1145/359340.359342
[19] Childs, A. M., & van Dam, W. (2010). Quantum algorithms for algebraic problems. Reviews of Modern Physics, 82(1), 1-52. https://doi.org/10.1103/RevModPhys.82.1
[20] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145–195. https://doi.org/10.1103/RevModPhys.74.145
[21] Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661–663. https://doi.org/10.1103/PhysRevLett.67.661
[22] Chen, J., Yang, Y., & Li, L. (2020). Post-quantum cryptography: Security and implementation. IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2020.2989961
[23] Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J. L. (2010). Quantum computers. Nature, 464(7285), 45-53. https://doi.org/10.1038/nature08812
[24] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484-1509. https://doi.org/10.1137/S0097539795293172
[25] Kiktenko, E. O., et al. (2018). Quantum-secured blockchain. Quantum Science and Technology, 3(3), 035004. https://doi.org/10.1088/2058-9565/aabc6b
[26] Renes, J. M. (2021). Quantum error correction and fault-tolerant quantum computing. Annual Review of Condensed Matter Physics, 12, 303-322. https://doi.org/10.1146/annurev-conmatphys-031620-103657
[27] Broadbent, A., Fitzsimons, J., & Kashefi, E. (2009). Universal blind quantum computation. 50th Annual IEEE Symposium on Foundations of Computer Science, 517-526. https://doi.org/10.1109/FOCS.2009.36
[28] Arrazola, J. M., & Lütkenhaus, N. (2014). Quantum fingerprinting with coherent states and a constant mean number of photons. Physical Review A, 89(6), 062305. https://doi.org/10.1103/PhysRevA.89.062305
[29] Cleve, R., Ekert, A., Macchiavello, C., & Mosca, M. (1998). Quantum algorithms revisited. Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 454(1969), 339-354. https://doi.org/10.1098/rspa.1998.0164
[30] Haner, T., Steiger, D. S., Svore, K. M., & Troyer, M. (2017). A software methodology for compiling quantum programs. Quantum Science and Technology, 2(3), 035003. https://doi.org/10.1088/2058-9565/aa7e6c
[31] Berta, M., Christandl, M., Colbeck, R., Renes, J. M., & Renner, R. (2010). The uncertainty principle in the presence of quantum memory. Nature Physics, 6(9), 659-662. https://doi.org/10.1038/nphys1734
[32] Van Meter, R. (2014). Quantum networking. Wiley.
[33] Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). Post-quantum cryptography. Springer. https://doi.org/10.1007/978-3-540-88702-7
[34] Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38-41. https://doi.org/10.1109/MSP.2018.3761723
[35] Rieffel, E. G., & Polak, W. H. (2011). Quantum computing: A gentle introduction. MIT Press.
[36] Brassard, G., & Fuchs, C. A. (1999). Cryptographic security from quantum mechanics: An introduction to quantum cryptography. SIGACT News, 30(2), 14-19. https://doi.org/10.1145/316896.316900
[37] Bennett, C. H., Brassard, G., & Ekert, A. K. (1992). Quantum cryptography. Scientific American, 267(4), 50-57. https://doi.org/10.1038/scientificamerican1092-50
[38] Boneh, D., & Lipton, R. J. (1995). Quantum cryptanalysis of hidden linear functions. Advances in Cryptology—CRYPTO '95, 424-437. https://doi.org/10.1007/3-540-44750-4_34
[39] Devitt, S. J., Munro, W. J., & Nemoto, K. (2013). Quantum error correction for beginners. Reports on Progress in Physics, 76(7), 076001. https://doi.org/10.1088/0034-4885/76/7/076001
[40] Lloyd, S. (1996). Universal quantum simulators. Science, 273(5278), 1073-1078. https://doi.org/10.1126/science.273.5278.1073



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY