1 TABLE OF CONTENTS

2 TO DO TASK 1: OUTLINE POST-QUANTUM COMPUTATIONAL LIMIT

In this technological era, with the advent of quantum computing technology, it aims to solve potential complex problems that are not able to be done by random computers. With the introduction of such technologies, it is likely to propose various post-quantum computational limits, security challenges, ethical and social concerns. In simple terms, quantum computers are working on the principles of quantum mechanics in order to perform all calculations in such a way that quantum bits are able to process vast amount of data (Rieffel et al., 2024). The main impact of such technologies is on cryptography where Shor's algorithm is being used to factorize large integers. In the post era, there are likely to be various computational limits due to immense increase of quantum computing technology in today's era. It is undeniable that quantum computers are able to excel specific tasks but could not be able to do various other tasks as of now. For example, it can be said that problems like database searching could be sped up with Grover's algorithm but it is quadratic which means it is not required for such scenarios. Instead of this, classical computers are suited best for such applications rather than focusing on the quantum advantages (Gill & Buyya, 2024).

There are even various challenges that could be faced with quantum computing based on development and scalability. This is because quantum computers are highly sensitive to different environmental disturbances which means there is a dire need for having an advanced error correction system along with

stable qubit architecture. As these metrics or applications are unavailable, it is likely to pose certain limitations on the quantum technology (Desdentado et al., 2024). This also represents that for the foreseeable future, both quantum computing and classical computing will coexist and will complement each other. Furthermore, in the case of research and development also for post-quantum computing, it is vibrant and is burgeoning at an exponential speed. In the coming future, there will be robust post quantum cryptographic standards just like RSA and ECC algorithms which could be used for standardizing the post-quantum cryptographic systems. Furthermore, there will be improved quantum algorithms available in the market which will make sure all potential security issues are patched and it is able to solve different types of problems. Finally, there will also be an appropriate quantum hardware available that would be able to overcome physical and engineering challenges that are being faced in today's world for constructing practical and scalable quantum computers (Stackpole, 2024).

There will be different ethical and social implications available that would have adverse impact on human beings. As quantum computing will be able to perform higher power computational, it means it will be able to break out today's existing cryptographic systems which could lead to the data privacy and security related issues. However, to avoid such things, there would be a need for ensuring a secure transition to the post-quantum cryptographic standards. Moreover, the use of such power can be misused by offenders in the case of surveillance and data analysis which must also be regulated. Henceforth, the post-quantum computing limits is not representing the end point but showing the new beginning where computation can be understood (Rieffel et al., 2024).

3 TO DO TASK 2: COMPARE PRESENT DAY COMPUTATIONAL LIMIT TO POST QUANTUM COMPUTATIONAL

The tabular matrix is attached below that clearly explains present day computational limit with respect to post quantum computational limit.

Aspect	Present Day Computational Limit	Post-Quantum Computational Limit
Cryptographic Security	In the current era, the cryptographic security mainly relies over RSA, ECC and other related algorithm, however, these algorithms are sometimes susceptible to classical attacks.	On the other hand, it mainly requires post-quantum cryptography i.e. lattice-based and code based which helps in resisting all types of quantum related attacks.
Algorithm Efficiency	In the context of classical algorithms, there are various tasks that are computationally infeasible such as factorizing of large numbers (Goldstein, 2023).	In the post quantum computational limit, the use of Shor's algorithm could be done in such a way that it will be able to make factorization feasible.
Speed	When it comes to speed, it is limited by classical transistor based hardware only.	However, in the case of quantum computing, its parallelism mainly offers the speedups for different problems like Grover's search algorithm.
Error Sensitivity	The error sensitivity rate for current limit is robust and even error rates can be manageable easily with current hardware resources.	In the case of post-quantum era, it is highly sensitive to environmental disturbances which means there would be a need for advanced error correction mechanisms.
Hardware Scalability	The hardware scalability is also possible in the current era with Moore's law that is approaching physical limits in the coming years.	The quantum computing hardware is still in early stages which means there would be significant challenges faced when qubits are to be scaled up.
Application Scope	Currently, the wide range of application are supported followed by optimization, machine learning and even data processing.	The quantum computers are perfect fit for higher complex tasks like optimization, natural science simulations and cryptographic operations.
Development Stage	It is well established and continuous increments are being made (Quantum News, 2024).	The field is evolving rapidly but still there are various challenges for quantum

		computing hardware, algorithms and software.
Ethical Considerations	The privacy and security could be maintained easily with current cryptographic standards available in the market.	The privacy and security could not be maintained easily with cryptographic standards as it can break currently available encryptions easily and there is no responsible use.
Integration	The current systems cannot combine with quantum computers as of now.	The hybrid systems can amalgamate with classical computers in an easy manner.
Future Outlook	In the future, the incremental improvements are approaching physical and theoretical limits for the classical computing.	Herein, the paradigm shift is seen for various advancements in the field of science and it can compete with classical computing easily (Quantum News, 2024).

4 TO DO TASK 3: IDENTIFY AND OUTLINE VULNERABILITIES IN PRESENT COMPUTATIONAL ABILITY AND CRYPTOGRAPHIC TECHNIQUES

Under this section, a detailed analysis will be performed on vulnerabilities that are primarily present in computational ability as well as cryptographic techniques.

4.1 COMPUTATIONAL LIMITS

The table attached below lists out all issues that are likely to be faced with quantum computing currently and in the coming years.

Issues	Description
Scalability Related Issues	• In the coming years, the transistor size is likely to approach the atomic scale which means the Moore's law will no longer will applicable. • Due to the increased processing power, there is an increased heat and the cooling technologies are likely to suffer.

	• For higher power consumption, it demands for higher energy that leads to sustainability related issues (S et al., 2024).
Algorithmic Efficiency	• There are certain problems that could be faced like factoring large integers and computing discrete logarithms which are not able to solve problems easily. • There are multiple problems classified like NP-hard and NP-complete which does not have polynomial time solutions. As a result of this absence, it is likely to limit solvability with classical methods available (Baker, 2023).
Processing Speed	• In the context of processing speed, it can be said that classical computers is able to process tasks sequentially as there is a limited speed and it cannot perform potential parallelism. • For the latency and bandwidth also, there are communication delays and limited data transfers with current systems.

4.2 CRYPTOGRAPHIC TECHNIQUES

Unlike computational problems, there are various vulnerabilities with cryptographic techniques which have been explained below in a tabular matrix.

Issues	Description
Algorithm Specific Vulnerabilities	• For the current encryption standard i.e. RSA, it is susceptible to factorization attacks which means it can be compromised. • For the ECC algorithm also, it relies over the discrete logarithm problems and it vulnerable to specific mathematical breakthroughs. • In the context of symmetric encryption, the use of techniques like AES are secure but is vulnerable to various attacks (S et al., 2024).
Key Management	• Key management is very essential in cryptography and it is challenging now as storage space can be compromised. • In the case of distribution and exchange also, there is a risk of interception. • The length of keys is short and poor which means it is vulnerable to brute forcing.

Implementation Flaws	• There are various vulnerabilities in cryptographic software and it can be exploited. For example, Heartbleed vulnerability • The risk of side channel attack is very high that results in timing attacks, power consumption and many more (Morstyn & Wang, 2024).
Social Engineering	• Owing to social engineering attacks, the cryptographic security can be compromised by deceiving all users into divulging sensitive information. • The insider threat is also possible which may allow accessing cryptographic keys easily.
Post Quantum Threats	• The post quantum threats are also possible where algorithms like Shor and Grover are likely to pose future threats based on current cryptographic standards. • The overall transition period is vulnerable because the quantum is able to compromise everything in the future (Morstyn & Wang, 2024).

5 REFERENCES

Baker, M. A. (2023, June 26). The environmental impact of Quantum Computing - Maher Asaad Baker - Medium. *Medium*. https://maher-asaad-baker.medium.com/the-environmental-impact-of-quantum-computing-386386990785

Desdentado, E., Calero, C., Moraga, M. Á., Serrano, M., & García, F. (2024). Exploring the trade-off between computational power and energy efficiency: An analysis of the evolution of quantum computing and its relation to classical computing. *Journal of Systems and Software*, 112165. https://doi.org/10.1016/j.jss.2024.112165

Gill, S. S., & Buyya, R. (2024). Transforming Research with Quantum Computing. *Journal of Economy and Technology*. https://doi.org/10.1016/j.ject.2024.07.001

Goldstein, P. (2023, October 17). What are the security implications of quantum computing? *Technology Solutions That Drive Business*. https://biztechmagazine.com/article/2023/10/what-is-quantum-computing-perfcon

Morstyn, T., & Wang, X. (2024). Opportunities for quantum computing within net-zero power system optimization. *Joule*. https://doi.org/10.1016/j.joule.2024.03.020

Quantum News. (2024, January 25). Quantum-Resistant FALCON algorithm challenges cryptography, promises secure IoT future. *Quantum Zeitgeist*. https://quantumzeitgeist.com/quantum-resistant-falcon-algorithm-challenges-cryptography-promises-secure-iot-future/

Rieffel, E. G., Asanjan, A. A., Alam, M. S., Anand, N., Neira, D. E. B., Block, S., Brady, L. T., Cotton, S., Izquierdo, Z. G., Grabbe, S., Gustafson, E., Hadfield, S., Lott, P. A., Maciejewski, F. B., Mandrà, S., Marshall, J., Mossi, G., Bauza, H. M., Saied, J., . . . Biswas, R. (2024). Assessing and advancing the potential of quantum computing: A NASA case study. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2024.06.012

S, B. K., A, S., M, M., Prasad, Y. J. D. S., & Ahmad, I. (2024). Quantum Computing Basics, applications and future Perspectives. *Journal of Molecular Structure*, 137917. https://doi.org/10.1016/j.molstruc.2024.137917

Stackpole, B. (2024, January 11). *Quantum computing: What leaders need to know now | MIT Sloan*. MIT Sloan. https://mitsloan.mit.edu/ideas-made-to-matter/quantum-computing-what-leaders-need-to-know-now