ISSN(O): 2320-5407 | ISSN(P): 3107-4928

International Journal of Advanced Research

Publisher's Name: Jana Publication and Research LLP

www.journalijar.com

REVIEWER'S REPORT

Manuscript No.: IJAR-58535

Title: Securing the Post-Quantum Era- Analyzing Quantum Threats, PQC Solutions, and Migration Challenges.

Recommendation:

Accept as it is .....

Accept after minor revision…yes.....

Accept after major revision .....

Do not accept (*Reasons below*) .....

Rating	Excel.	Good	Fair	Poor
Originality			Y	
Techn. Quality			Y	
Clarity			Y	
Significance			Y	

Reviewer's ID: JPR-Dr.Shaweta Sachdeva

Detailed Reviewer's Report

MAJOR COMMENTS

1. The paper does not clearly state its research question, objective, or contribution. What is new compared to existing surveys,,?[9][23][24]
2. Add a paragraph at end of Introduction stating: objective, methodology of review, and what this survey adds.
3. Add a comparison table of existing surveys vs your work.

1. Structural Issues

4. No Abstract keywords, No Introduction heading - starts abruptly.
5. Section flow is weak. Suggest standard structure: Abstract, Keywords, 1. Introduction, 2. Background (RSA/ECC vulnerability, Shor's/Grover), 3. Families of PQC, 4. NIST Standardization Process, 5. FIPS 203/204/205 - ML-KEM, ML-DSA, SLH-DSA, 6. Challenges in Migration, 7. Future Directions, 8. Conclusion.
6. The Discussion from lines 366-382 about blockchain, 6G, ZTA, QKD is interesting but not elaborated anywhere else. Either expand with citations or remove.

2. Technical Depth is Missing

7. Lines 385-390: Statement "RSA and ECC will be breakable" is correct but needs quantitative analysis. Add timeline estimates, qubit requirements - you cited Gidney & Ekerå but didn't discuss it.[16]
8. No technical comparison of lattice vs code-based vs multivariate vs isogeny vs hash-based. Add a table: Security Assumption, Key Size, Signature Size, Performance, NIST Status.

ISSN(O): 2320-5407 | ISSN(P): 3107-4928
International Journal of Advanced Research
Publisher's Name: Jana Publication and Research LLP
www.journalijar.com

REVIEWER'S REPORT

9. No mention of why SIKE / Isogeny was broken in 2022 - important lesson for "single point of failure" argument you make in L369-371.

3. NIST Update Inaccurate / Outdated

10. You mention ML-KEM, ML-DSA, SLH-DSA correctly, but in text still refer to old names CRYSTALS-Kyber/Dilithium. Clarify: ML-KEM is standardized as FIPS 203 (formerly Kyber) [Ref 7, 17], ML-DSA is FIPS 204, SLH-DSA is FIPS 205.

11. Falcon is missing - NIST selected Falcon as additional signature.

12. References to 2026 [Refs 14, 15, 16, 25, 26] look like future-dated / predatory whitepapers. Replace with authentic peer-reviewed sources. Palo Alto Networks blog is not a scholarly source.[15]

4. References - Serious Formatting Issue

13. Duplicate references: and are identical NIST IR 8105, 2016.[2][6]

14. L. K. Grover, "A Fast Quantum..." in Proc. 28th Annu. ACM Symp. Theory... - incomplete proceedings name (STOC).[4]

15. Inconsistent format: Some have DOI, some don't. Volume, page numbers missing for many.

16. Too many non-academic sources: Quantropi White Paper, Stormshield blog, AWS re:Inforce. Reduce to <10% grey literature.[14][27][29]

17. References,,, are 2023-2025 - check if they are actually published. Provide DOI links.[9][10][11][12]

MINOR / LANGUAGE COMMENTS

1. Grammar and Language - Needs extensive proofreading:

18. L366-368: "Really, present standardized algorithms, although very secure, often require high computational and memory resources which Really constrain..." - Remove "Really", fix capitalization.

19. L385-386: "Quantum Computing The introduction of quantum computing has potential to..." - Sentence fragment.

20. L393: "Luckily, the cryptographic community has not only reacted rapidly but also has worked closely and intensively." - Informal word "Luckily" - use "Notably" or "Importantly".

21. L397: "Yet, the piece also highlights that we are a long way from the finish line" - Very informal for a review paper.

22. L404-406: Last sentence is convoluted. Rewrite.

23.Define PQC, QKD, 6G, ZTA, HNDL (Harvest Now Decrypt Later), ECC, RSA at first use.

24. It repeats introduction. It should summarize findings, limitations of current PQC, and concrete future research agenda (crypto agility, hybrid deployment, side-channel resistance L373-375).

25.Currently no figures or tables. A survey without a single architecture diagram or timeline of NIST process (2016-2024) is weak. Suggest adding at least 2 figures: NIST PQC timeline, and Classification of PQC families.