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.....
Accept after major revision ...✓.....
Do not accept (*Reasons below*) .....

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

Reviewer's ID: JPR- **098**

Detailed Reviewer's Report

Decision: Accept after Major Revision

Summary:

The manuscript addresses a highly relevant topic in cybersecurity: the transition from conventional public-key cryptography to Post-Quantum Cryptography (PQC). It reviews quantum threats, NIST-standardized PQC algorithms, migration challenges, and hybrid cryptographic approaches. The paper also includes a computational experiment comparing classical, PQC, and hybrid key exchange mechanisms. The topic is timely and important because organizations worldwide are preparing for quantum-safe cryptographic migration.

The paper is informative and easy to follow, but it contains several methodological and presentation issues that should be addressed before publication.

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

Strengths

1. Timely and Important Topic

The manuscript focuses on one of the most active research areas in cybersecurity.

The discussion on

- Quantum threats
- Harvest Now, Decrypt Later attacks
- NIST PQC standards
- Hybrid cryptography
- Migration strategies

is relevant and useful.

2. Comprehensive Literature Review

The literature survey summarizes important developments from

- Shor's Algorithm
- Grover's Algorithm
- NIST PQC competition
- Kyber
- Dilithium
- SPHINCS+
- Hybrid cryptography

The review provides a good background for readers entering the field.

3. Practical Perspective

Unlike many review papers, this manuscript attempts to validate the discussion through a computational experiment involving X25519 and ML-KEM. The inclusion of execution time, handshake latency, and hybrid overhead adds practical value.

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

4. Good Organization

The manuscript follows a logical structure:

- Introduction
- Problem Statement
- Literature Review
- Quantum Threat
- PQC Solutions
- Open Challenges
- Methodology
- Validation
- Future Work
- Conclusion

This improves readability.

Weaknesses

1. Limited Novelty (Major Issue)

The paper is primarily a **survey combined with a small validation study**.

Most technical content is summarized from existing NIST publications and previous literature.

The paper does **not introduce**

- a new PQC algorithm,
- a new migration framework,
- a new protocol,
- a new optimization technique.

The experimental section mainly validates existing knowledge rather than providing new scientific contributions.

2. Methodology Needs Better Justification

The computational experiment requires additional details.

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

Although the manuscript mentions a **10,000-record simulated dataset**, the paper does not sufficiently explain

- how the dataset was generated,
- whether measurements were entirely simulated,
- what assumptions were made,
- reproducibility of the simulation.

These details are necessary for scientific reproducibility.

3. Statistical Analysis

Welch's t-test is reported.

However,

- confidence intervals,
- effect sizes,
- sensitivity analysis,

are not presented.

These would strengthen the statistical validity.

4. Experimental Evaluation

The experimental validation focuses only on

- X25519
- ML-KEM

The paper would be significantly stronger if additional NIST-standardized algorithms (e.g., ML-DSA or SLH-DSA) were evaluated under similar conditions.

5. Figures

Several figures are relatively simple and appear to summarize existing concepts rather than present original findings.

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

Higher-quality figures with clearer captions and interpretation would improve the presentation.

6. Writing Quality

Numerous grammatical and stylistic issues remain throughout the manuscript.

Examples include:

- inconsistent spacing,
- capitalization errors,
- awkward sentence construction,
- repeated wording,
- punctuation inconsistencies.

The manuscript would benefit from professional English proofreading.

7. References

Although the reference list is extensive, several citations are

- white papers,
- organizational reports,
- vendor publications.

Minor Comments

- Define abbreviations consistently at first use.
- Improve the quality and readability of all figures.
- Include hardware specifications for experiments.
- Clearly distinguish between measured and simulated results.
- Add a comparison table summarizing classical cryptography, PQC, hybrid cryptography, and QKD.
- Improve formatting consistency across tables and captions.
- Reduce repetition between the "Open Issues" and "Proposed Solutions" sections.

Overall Recommendation

Recommendation: Accept after Major Revision

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

The manuscript addresses an important and timely topic with practical relevance to the cybersecurity community. Its strengths include a comprehensive overview of post-quantum cryptography, discussion of migration strategies, and a practical evaluation of hybrid key exchange mechanisms. However, the work is largely a synthesis of existing research, and the experimental contribution is limited. The methodology requires additional detail for reproducibility, the statistical analysis should be strengthened, and the manuscript would benefit from substantial improvements in language, presentation, and experimental depth. Addressing these issues would significantly improve the paper's scientific quality and impact.