



Task 8 “Hybrid Post-Quantum Cryptographic Framework for Secure and Efficient IoT and Cloud Systems”

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (3)

Task 8

Introduction

السلام عليكم

In this presentation, I will propose a doctoral research project in the field of cybersecurity, more precisely in cryptography and new technologies. This proposal is built from a critical analysis of the gaps identified in recent scientific literature.

2. Issue

With the emergence of quantum computing, classical cryptographic systems are becoming vulnerable.

Post-quantum cryptography solutions exist, but they still present:

- ☐ performance issues
- ☐ difficulties integrating into IoT systems
- ☐ a lack of validation in real-world environments

Thus, the problem is:

→ How to design a hybrid cryptographic model that is secure and efficient, adapted to the constraints of IoT and cloud environments?

3. Identification of research gaps

In accordance with the professor's remarks, the gaps are classified into three categories:

❑ A. Theoretical Gaps

- Absence of a unified framework combining classical and post-quantum cryptography
- Lack of well-formalized hybrid models

❑ Scientific support:

The work of the National Institute of Standards and Technology on post-quantum cryptography shows that the standards are still being stabilized.

⚡ B. Methodological gaps

- Few studies use a rigorous comparative approach
- Low use of multi-environment validation (IoT + cloud)

❖ **Reference:** The studies by Bernstein et al. show a lack of complete experimental validation.

C. Practical Gaps

- ❑ Difficulty of implementation in IoT systems
- ❑ High computational cost of post-quantum algorithms

Important:

These elements are distinguished as practical gaps and not just as technical limitations.

4. Research objectives

Main objective:

→ Develop a secure and efficient hybrid cryptographic model for IoT and cloud systems.

Specific objectives:

1. Design a hybrid architecture (classical + post-quantum)
2. Evaluate the performance of algorithms
3. Reduce computational cost
4. Test the model in simulated and real environments

5. Research questions

- 1) Do hybrid models improve security against quantum attacks?
- 2) What is the impact on performance in IoT systems?
- 3) How can the balance between security and efficiency be optimized?

6. Methodology

The research adopts a sequential multi-method approach.

Steps:

- 1) Systematic literature review
- 2) Design of the hybrid model
- 3) Implementation in a simulation environment (CloudSim, IoT testbed)
- 4) Experimentation
- 5) Statistical analysis:
ANOVA (multi-group comparison)t-test
(comparison between models)

7. Methodology link ↔ gaps

- ❑ Theoretical gaps are addressed through the design of the hybrid model
- ❑ Methodological gaps are addressed through rigorous
- ❑ comparative validation Practical gaps are addressed through tests in a real environment
- This strengthens the internal coherence of the research.

8. Expected results

- ❖ Improvement of security against quantum attacks
- ❖ Reduction of computational cost
- ❖ Adaptability to IoT systems
- ❖ Decrease in vulnerabilities

9. Critical Evaluation

✓ Expected strengths:

innovative approach strong theoretical and practical contribution

✗ Risks:

- model complexity
 - dependence on test environments
- The proposed methodology generally addresses the gaps, but its effectiveness will depend on actual experimental validation.

10. Scientific contribution

This research will contribute to:

- filling theoretical gaps (hybrid model)
- improving experimental methods
- proposing solutions applicable in real-world contexts

CONCLUSION

In conclusion,

This research proposal addresses the gaps identified in the literature on cryptography and cybersecurity.

It proposes an innovative approach combining security, performance, and adaptability to new technologies.

It thus constitutes a relevant contribution to the future development of cybersecurity.

Thank you for your attention.

Assalamu Alaikum.

- 1) National Institute of Standards and Technology (2022) Post-Quantum Cryptography Standardization
- 2) Bernstein, D. J., et al. (2017)
- 3) Post-Quantum Cryptography
- 4) Chen, L., et al. (2016) NIST Report on Post-Quantum Cryptography
- 5) Alkim, E., et al. (2016) NewHope Cryptosystem



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank you!!!

