



Task 9 “Critical Evaluation of Lattice-Based Cryptography Theory in Post-Quantum Cybersecurity Research”

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (3)

Task 9

Introduction

السلام عليكم

In this presentation, I will critically analyze a PhD thesis in cybersecurity, focusing on the scientific theory used, its critical evaluation, and my personal position.

1. Presentation of the thesis

The chosen thesis is: "Lattice-Based Cryptography for Post-Quantum Secure Communications"

Author: Daniel J. Bernstein

University: Eindhoven University of Technology

Year: 2017

This thesis falls within the field of post-quantum cryptography, which aims to secure communications against attacks from quantum computers.

2. Scientific theory used

The thesis is mainly based on the following theory:

Theory of Euclidean networks (Lattice-Based Cryptography)

This mathematical theory is based on:

- ❑ problems that are difficult in lattices
- ❑ like the shortest vector problem (SVP)
- ❑ and the closest vector problem (CVP) These problems are considered:
→ difficult to solve even with quantum computers

Scientific reference

The work is supported by research from the National Institute of Standards and Technology, which recommends network-based algorithms as primary candidates for post-quantum cryptography.

3. Critical analysis of the theory

Strengths of the theory

1. Resistance to quantum attacks

→ Unlike RSA, this theory remains secure against quantum algorithms.

2. Solid mathematical foundation

→ Based on well-studied and recognized hard problems.

3. International adoption

→ Used in emerging NIST standards.

✗ Limitations of the theory

- 1) High computational complexity
→ Calculations are heavy, especially for IoT systems.
- 2) Large key size
→ Can be problematic for storage and transmission.
- 3) Difficult implementation
→ Requires advanced optimizations.

In-depth critical analysis

Although the theory is mathematically sound, it has a significant limitation:

→ it favors theoretical security at the expense of practical performance.

This creates an imbalance between:

- ☐ high security
- ☐ and real-world applicability

4. Link theory $\leftrightarrow$ methodology $\leftrightarrow$ results

The thesis uses:

- a formal mathematical approach
- followed by experimental implementations

→ This methodology allows:

- validating the theory
- testing its performance

Observed results:

enhanced security but reduced performance

→ This directly confirms the identified theoretical limits.

5. Personal position (agreement or disagreement)

My position:

I partially agree with this theory.

✓ Points of agreement

- ☐ It is essential for preparing for the future in the face of quantum threats
- ☐ It represents a major advancement in cybersecurity

✗ Points of disagreement

I consider that:

→ the theory is not yet adapted to real environments

notably:

- ❖ IoT
- ❖ embedded systems
- ❖ resource-limited infrastructures

Justification

A scientific theory must be:

- ☐ secure ✓
- ☐ but also applicable and optimized

However, here:

→ performance remains a major obstacle

Critical proposal

To improve this theory, I propose:

- 1) Develop hybrid models
→ combine classical and post-quantum cryptography
- 2) Optimize algorithms for IoT
- 3) Test in real environments

CONCLUSION

In conclusion,

The theory of networks applied to post-quantum cryptography constitutes a solid scientific foundation for future cybersecurity.

However, it has significant limitations in terms of performance and applicability.

Thus, although I recognize its scientific value, I believe it needs to be improved to meet the real needs of modern systems.

Thank you for your attention.

Assalamu Alaikum.

- 1) National Institute of Standards and Technology (2022)
Post-Quantum Cryptography Standardization Project
- 2) Bernstein, D. J., et al. (2017) Post-Quantum Cryptography
- Micciancio, D., & Regev, O. (2009) Lattice-based Cryptography



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank you!!!

