ÉCOLE NATIONALE SUPÉRIEURE D'ARTS ET MÉTIERS
UNIVERSITÉ HASSAN II DE CASABLANCA

Master's Degree - 2nd Year
Big Data and Internet of Things
Academic Year 2024-2025

Progress Report #2

Optimization of IoT Communications through Compression and Lightweight Post-Quantum Cryptography

Student:
Abdessamad JAOUAD
M2 Big Data & IoT

Supervisor:
Prof. Ibrahim GUELZIM
ENSAM Casablanca

December 2025

1 Introduction

This is the second progress report for my research project on **"Optimization of IoT Communications through Compression and Lightweight Post-Quantum Cryptography"**. This report covers the period from December 11 to December 27, 2025.

The project focuses on investigating how Post-Quantum Cryptography (PQC) algorithms have been adapted for resource-constrained IoT devices. The goal is to produce a concise, accessible research survey that explains PQC for IoT without excessive mathematical complexity.

2 Work Completed

2.1 Research on NIST-Standardized PQC Algorithms

I conducted in-depth research on the four main NIST-standardized post-quantum algorithms:

- **ML-KEM (Kyber)**: Key Encapsulation Mechanism based on Module-LWE, standardized as FIPS 203
- **ML-DSA (Dilithium)**: Digital Signature Algorithm based on Module-LWE/SIS, standardized as FIPS 204
- **SLH-DSA (SPHINCS+)**: Hash-based signature scheme, standardized as FIPS 205
- **Falcon**: Compact NTRU-lattice-based signatures (upcoming standard)

I focused particularly on **lattice-based algorithms** (Kyber, Dilithium, Falcon) as they offer the best balance of security and performance for IoT applications.

2.2 Key Insights Gained

2.2.1 Algorithm Characteristics

I learned the key differences between the algorithms, including their key sizes, signature sizes, and performance trade-offs:

Algorithm	Type	Public Key	Signature/Ciphertext
ML-KEM-768	KEM	1,184 B	1,088 B
ML-DSA-65	Signature	1,952 B	3,293 B
Falcon-512	Signature	897 B	666 B
SLH-DSA-128s	Signature	32 B	7,856 B

Table 1: Comparison of PQC algorithm sizes (NIST Level 2/3)

2.2.2 Why Lattice-Based Algorithms are Preferred for IoT

I understood why lattice-based schemes are the leading choice for IoT:

- Efficient polynomial operations via Number Theoretic Transform (NTT)
- Reasonable key and signature sizes (compared to code-based or hash-based)
- Good performance on ARM Cortex-M class microcontrollers
- Well-studied security foundations (LWE, SIS problems)

2.3 Lightweight Optimization Techniques

I researched how PQC algorithms are optimized for constrained IoT devices:

- **NTT optimization**: Fast polynomial multiplication reducing complexity from $O(n^2)$ to $O(n \log n)$
- **Memory management**: In-place operations, buffer reuse, streaming hash computation
- **Role-based design**: IoT devices only verify signatures; servers handle signing
- **Hardware acceleration**: Leveraging AES-NI and SHA accelerators when available
- **Parameter selection**: Using lower security levels (NIST Level 1) when appropriate

2.4 IoT Constraints Analysis

I studied the specific constraints of IoT devices and their implications for PQC:

Device Class	RAM	PQC Feasibility
Class 0 (Sensor nodes)	<10 KB	Very limited
Class 1 (Smart meters)	∼10 KB	Limited (verify only)
Class 2 (Wearables)	∼50 KB	Feasible with optimization
Class 3 (Gateways)	>256 KB	Full PQC support

Table 2: IoT device classes and PQC compatibility

2.5 Document Writing Progress

I made significant progress on writing my research survey:

- Created the **document outline and structure**
- Wrote **introduction and overview sections**
- Drafted sections for all four main algorithms (Kyber, Dilithium, SPHINCS+, Falcon)
- Wrote about **IoT constraints** and how PQC addresses them

The document is designed to be concise and accessible, focusing on practical insights rather than heavy mathematical details.

3 Challenges Encountered

1. **Mathematical complexity**: Understanding the underlying mathematical concepts (lattices, LWE, SIS, polynomial rings) required significant effort
2. **Algorithm derivation**: Connecting the abstract mathematical problems to the concrete algorithm implementations was challenging
3. **Balancing depth vs. accessibility**: Finding the right level of detail for a practical survey without oversimplifying, or overwhelming the reader with the mathematical details

4 Next Steps

The final report is due on the week of **January 5, 2026**. The remaining tasks are:

1. **Benchmark research**: Study real performance data from pqm4 project and academic papers
2. **Library exploration**: Document available PQC libraries (liboqs, PQClean, pqm4, wolfSSL)
3. **Comparison tables**: Create comprehensive comparison tables for the survey
4. **Document completion**: Finalize all sections and polish the writing
5. **Final review**: Proofread and prepare for submission

5 Conclusion

During this reporting period, I have made substantial progress on both the research and writing aspects of my project. I now have a solid understanding of the main NIST-standardized PQC algorithms, their optimization techniques for IoT, and the constraints of embedded devices.

The next phase will focus on incorporating real benchmark data and completing the final version of my research survey before the January 5th deadline.

Submitted by: Abdessamad JAOUAD
Date: December 27, 2025
Supervisor: Prof. Ibrahim GUELZIM