Firat Donmez
Pavla Dimitrova
Eindhoven, The Netherlands

Fontys University of Applied Sciences

Project Proposal
Implementation of Ring-LWE and NTT-Optimized Ring-LWE

During the recent decades, quantum technology has exponentially improved, putting us in danger of the collapse of current cryptographic systems. This also applies to the communication between an earth base and a space station or satellite, as those types of spacecrafts are designed to remain in orbit for multiple decades, making them perfect for the HNDL(harvest now, decrypt later) attacks. Within this project we will focus on post-quantum cryptography as a means of defence in this specific scenario.

In this scope of work, we will focus on ensuring **high speed and data integrity** for issuing commands from the earth base to the spacecraft, such as orbit adjustment thruster commands. It is vital that those commands arrive and are encrypted and decrypted fast, and that no data gets lost or corrupted. We will also focus on **processing power and energy usage** due to the limited energy supply and processing power of a spacecraft. We will try to acquire or at least mimic CCSDS packets(Consultative Committee for Space Data Systems) for our data. We plan to contact ESA and NASA to request real or mock satellite communication datasets, but we will use the NIST Post-Quantum Cryptography for benchmarking as a fallback.

We will perform two main steps. First of all, the algorithmic implementation of the Ring-LWE scheme using polynomial multiplication and the NTT-based multiplication to improve efficiency in computation will be followed. The second step consists of performance evaluation by comparing execution time and memory usage and integrity. We will use the course materials as a starting point for our implementation as those algorithms were covered during class. The algorithm we will implement requires smaller keys and is quite fast, making it fitting for our space-station scenario.

The research questions we will focus on are:

1. How much does the NTT-based multiplication reduce the execution time compared to standard polynomial multiplication when processing large data blocks?
2. What is the difference in memory usage between the standard and NTT-optimized versions?
3. Does optimization negatively affect data integrity upon decryption?

We will implement Ring-LWE in Python, leveraging libraries like timeit and memory profilers to measure key performance indicators (KPIs). Our approach will combine mathematical optimization (e.g., Cooley–Tukey for NTT) with software testing to ensure we meet security standards are met while avoiding security-weakening steps.

Our project goal is to gain practical insight into algorithmic optimization, specifically the efficiency impact of NTT, and contribute to the understanding of computational indicators in post-quantum cryptography.