APPENDIX D — ANALYSIS OF SENIOR PROJECT DESIGN

Project Title: Post-Quantum Encryption Benchmark

Student's Name: Jordan Churi
Student's Signature:

Advisor's Name: Dr. Callenes-Sloan
Advisor's Initials: Date:

- **Summary of Functional Requirements**

Implement benchmarks of several post-quantum encryption protocols using rLWE.

- **Primary Constraints**

The limiting factors that impacted this project are the dependency on OpenSSL for all the different implementations of the post-quantum encryption algorithms. Other aspects that made this project challenging was trying to implement this on an MSP432P401R as I discovered the MSP432P401R was missing some development kits to implement these encryptions.

- **Economic**

The economic impacts of this project are enormous; encryption is the underpinning of all online systems like online banking or any online business. Though this project does not have a life cycle, these encryption protocols will change as the NIST search for a post-quantum encryption standard continues. Additionally, at this time, any information towards selecting the candidates that make it to round three has implications on who shapes the future of encryption.

- **Environmental**

The ethical implication of this project is the energy usage depending on how much time the encryption takes to encode and decode data. This is because the longer it takes to run this program, the more energy it will use. This increase in time, especially when there are millions of devices can have a significant impact on the environment due to energy generation.

- **Manufacturability**

No issues with manufacturing as this project implemented in software.

- **Sustainability**

This project impacts the sustainable use of resources because making the most efficient encryption algorithm is vital to use the least amount of energy as possible. Additionally, selecting a good standard now is essential because, in the future, more secure cryptosystems are most likely to be built off of this encryption.

- **Ethical**

The ethical implication of this project is if there is a security flaw in the encryption algorithm and it was knowingly not mentioned, it would leave a backdoor into people's communication causing their privacy to be violated.

- **Health and Safety**

A safety concern with this project is the use of encryption for medical purposes.

- **Social and Political**

Some social and political issues associated with this project is that encryption is used for groups to communicate with each other without the view of external groups like governments and corporations. The use of encryption is critical for keeping personal data personal.

- **Development**

Some new things that I learned over the development of this project are Post-Quantum Encryption protocols, current asymmetric key exchange, and OpenSSL.