Ryan Christopher
MET CS566
Project Proposal

An Examination of Lattice-based Cryptography through the Kyber Algorithm

As quantum supremacy inches closer to reality, public key systems demand new methods to preserve security in the presence of quantum computers. The National Institute of Standards and Technology (NIST), announced the first four quantum-resistant cryptographic algorithms in 2022, where CRYSTALS-Kyber was named for general encryption.

The Kyber algorithm differs from existing public key methods such as RSA and ECC as it employs the use of lattice-based cryptography to generate public and private keys in the forms of vectors in a multi-dimensional matrix. According to the CRYSTALS website, Kyber's "security is based on the hardness of solving the learning-with-errors (LWE) problem over module lattices" achieving security against known classical and quantum attacks.

This project will focus on how the Kyber algorithm generates keys, encrypts data, and decrypts data, in addition to performing an analysis on the efficiency of the algorithm compared to an existing and widely used public key method such as RSA. This will take into account the time it takes to generate keys, key sizes, and the time required to encrypt and decrypt a variety of examples of data to gain a better understanding of how post-quantum cryptographic algorithms can be used on classical machines.

The following libraries allow for both Kyber and RSA to be implemented through the Rust language:

Rust crate pqc_kyber: https://docs.rs/pqc_kyber/latest/pqc_kyber/index.html

Rust crate rsa: https://docs.rs/rsa/latest/rsa/

Working with this algorithm is particularly interesting to me as I believe that it will be necessary for secure communication in the near future as quantum chips such as IBM's Heron, Google's Willow, and Microsoft's Majorana achieve higher qubit counts, improved error correction, and longer states of operation.

Resources:

Lima, Ribeiro, Queiroz, Quintino, Silva, Santos, Roberto "Evaluating Kyber post-quantum KEM in a mobile application" *NIST*, https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/ribeiro-evaluating-kyber-pqc2021.pdf

Gonzales, Ruben, "Kyber – How does it work?", *Approachable Cryptography*, https://cryptopedia.dev/posts/kyber/