The Cost of the Quantum Transition

Joshua Deckman & Jack Pearson

Project Vision

- Evaluate costs of preparation for Y2Q
  - Compare pre-quantum asymmetric crypto & post-quantum asymmetric crypto
    - ECC vs Kyber
- Produce comparable pre-quantum & post-quantum programs and evaluate their performance in extreme conditions
- We anticipate increased network requirements will be the bottleneck

Hardware, Toolchain, and Details

The project will be implemented with Rust on a Raspberry Pi. In a series of tests, the Raspberry Pi, acting as a network server, will perform both Kyber and elliptic curve key exchanges with a client, tracking the processing cost, latency, and bandwidth associated with each exchange.

Deliverables

- Kyber & ECC key exchange software (Rust)
- Benchmark harness software (rate limiting, network latency simulation)
- Benchmark data (key exchange latency vs bandwidth & vs network latency)
- Plots
- Final report