Performance and Operability of Post Quantum Cryptography Algorithms on Resource Constrained IoT Devices

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Introduction

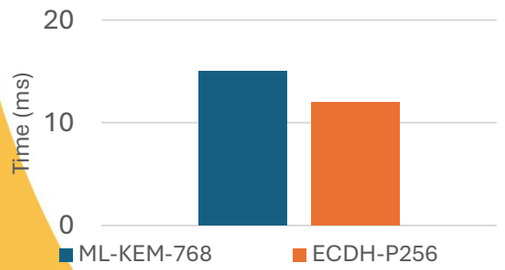
There will always be an innovative technology that replaces or makes its predecessor obsolete. Encryption algorithms are no stranger to this concept, and organizations are now preparing for the next age of encryption for quantum computers. The threat of large-scale quantum computers poses a significant threat to modern encryption.

Problem & Motivation

Problem: IoT Devices have a limited CPU, memory and energy available to them. Current encryption methods are under threat of being broken by quantum computers.

Question: Can leading PQC Algorithms, such as ML-KEM & ML-DSA run efficiently on constrained hardware.

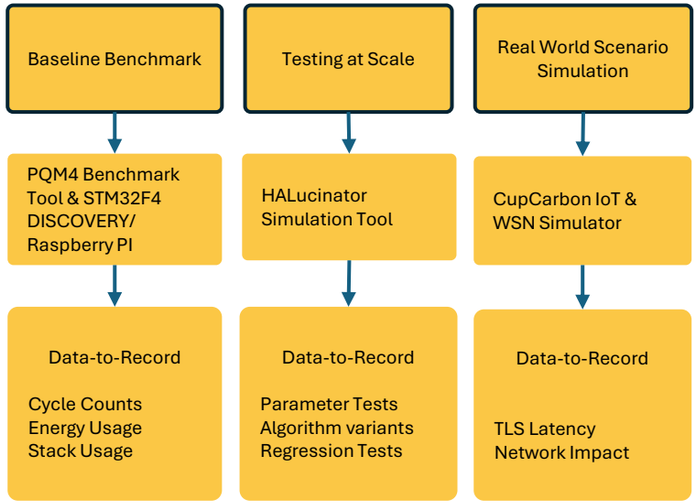
Goal: Provide quantitative data that shows the performance of PQC algorithms on constrained IoT devices.



Key establishment latency comparison between ML-KEM and ECDH on a resource constrained IoT device.

Methodology

The methodology will contain three steps for gathering data



Algorithms Under Test

The algorithms being evaluated consist of leading PQC algorithms and leading current encryption algorithms.

Proposed PQC and current encryption algorithms:

- ML-KEM
- ML-DSA
- ECDH
- ECDSA

Each algorithm will be run multiple times against different parameters and then compared against the others

Key Metrics

Performance will be evaluated across four different categories in order to gather the most complete picture.

Cryptographic Operations
- Sign/Verfiy Cycles
- Encap/Decap Cycles

Memory
- Stack Usage
- Ram Usage

Energy Consumption
- Draw form cycles
- Battery Longevity

Network & TLS Performance
- TLS Latency
- End-to-end delay

STM32F4 DISCOVERY

Raspberry PI

What's Next

From here the remaining work will be to take the proposed methodology and perform the testing over a number of steps.

- Set up testing environment
- Algorithm performance data
- Comparison of results
- Create graphs and visuals to present data

setu.ie

Contact: Liam Halliden
Email: C00326176@setu.ie