Informatik Projekt 2

Post Quantum Cryptography on Raspberry Pi

12mojo1bif@hft-stuttgart.de
12test11bif@hft-stuttgart.de
12test21bif@hft-stuttgart.de

Group: 4

Group Members:
Jonas Möwes, Ayham, Omar

2025-02-01

Contents

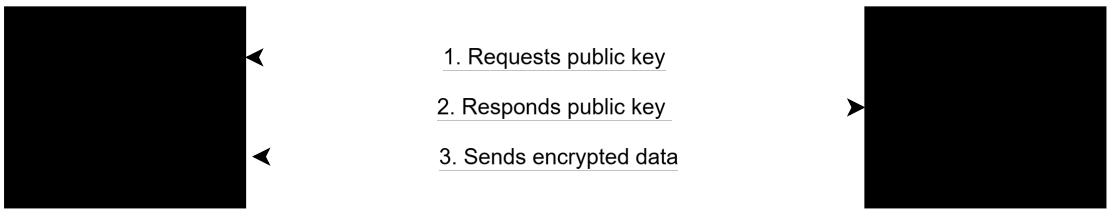
1 Introduction

In this project we explored the efficency of Post Quantum Cryptography (PQC) Algorithms on Microcontroller. To measure this we wanted to create a benchmark that tests these with real data. In the beginning we tried to run these algorithms on very lightweight systems like an ESP32 or even an ESP8266. See (Doc) for further Information.

This document will set the Focus on what the results of the finished project accomplished.

After we realized that it wont be as easy as thought to run PQC algorithms on these very lightweight systems we decided to focus on the Raspberry Pi implementation. The implementation of the benchmark changed alot over the time of this project but always had the goal to create a real scenerio on how a embedded system would publish its data to a server while this beeing Post Quantum safe. The Realisation section goes over some mid level implementations.

Broken down to the communication of the server and client it comes down to this sequence:



2 Realisation

Previous implementations:

3 Further Details

4 Evaluation

5 Conclusion