Project notes

- Deconstructed baby kyber to undestand kyber encryption mechanism.
- Researched & undestood Key encapsulation Mechanism (KEM)
- Implemented kyber on STM 32 board, Sucessfully ran test_kyber to test KEM.

Questions:

What to benchmark?

- Key exchange as seen in test_kyber
- encryption & decryption.

code needed to port kyber:

✓ Kem.h
✓ Params.h
indcpa.h
verify.h
Symmetric.h
randombytes.h

✓ Polyvec.h
✓ Poly.h
✓ ntt.h

✓ reduce.h
✓ cbd.h