Project Notes

Meeting 04/12/23

- Can use PQM4 library ✓
- Which kyber to use 512? ✓
- ARM M4 optimized Ascon exists
- Benchmarks - key exchange or encryption/decryption
- Initial demo

KEM
{ Key gen
encapsulation
decapsulation. }

Demo - Replace key gen
Algo with Ascon

5th Jan

22/12/2023

Demo is to replace key gen with Aman & benchmarks

on 5/01/2024

11/01/2024 - demo slot.

ppt demo /

i.e.

Short Presentation & demo of running code.