1. The simulation work of fault on NTT has been done on Newhope, kyber, and dilithium. This work based on pqm4 library implementation for ARM Cortex-M4. By skipping the load instruction of ‘twiddle-ptr’.
2. The physical experiment may need to be done after ravi could access to the lab and check the vulnerability. Besides, we can check if PFA could be used on this model.
3. The previous discussion is about implementations of PQC on ARM. Considering liboqs library, the same attack method could be applied on software implementations, using rowhammer etc. to inject fault.