1.针对pqm4库中的newhope, kyber, dilithium算法中的NTT操作进行fault attack in simulation by gdb debugger.

仿真是通过修改编译得到的二进制文件，将二进制文件中写好的地址进行修改后，再对修改后的文件执行debug。

对这三种算法进行仿真的攻击，针对key generation, encapsulation, decapsulation, sign, verify各模块中调用到NTT的部分进行分析。

如果要做physical attack， 他偏向于他们实验室之前提到的,在从flash中load数据的过程中，可以对某个数据进行篡改。但是现在他们无法去实验室，所以并没有进行这方面的后续工作。

也提到是否可以参考PFA等等其他故障工作来进行故障攻击。我的想法是，可以看看这个常数有没有预存。如果没有，那么就是在执行期间从flash中load到寄存器中。

2.ravi提到他在看liboqs库。他先初步看了下，说我们也可以看看。如果NTT实现方案一致或类似，那么可以尝试用rowhammer等等方式来进行软件的FA。