# Hardware NTT Acceleration for CRYSTALS-Dlithium

## CRYSTALS-Dlithium NTTxINTT Accelerator base on software, supposedly work with AXI and External memory (to share with RISC-V cache)

Expect to add support for CRYSTALS-Kyber 16-bit

* Status:
  + Only done the butterfly unit (pipelined 5 clock)
  + Expect to fetch data from a FIFO ctrl (with BRAM)

A black and white diagram

Description automatically generated

Figure 1 Current BU

* What’s left:
  + Scheduler
  + Way to fetch NTT data from external memory
* Working on:
  + So we need a number of BU, expect to use 32 for start and scale up. Each operation needs an index and feed data directly. Expect data feed to each BU (2-input) to be:
    - Input: index + op + imm1 + imm2
    - Output: index + op + rslt1 + rslt2
    - By leaving the loop index