Verification Report

This project works for 2 parameter sets “mayo1” and “mayo2”

I have implemented a software code in c to generate intermediate test vectors like expanded public key, signature, target from official mayo-c software implementation. It is named as “**verify_val_gen.c**”. When it is executed, it generates a text file named “**input_file.txt**”

I have implemented another software code in JS, to generate final test vectors. I implemented the whole mayo verify algorithm in JS and the resultant vector along the expanded public key and signature is written into a text file as output when executed. Implemented is named as “**mayo.js**” and when it is executed, it generates text files named “**input_gen_mayo1_file.txt**” or “**input_gen_mayo2_file.txt**”, based on setting the type “**mayo1**” or “**mayo2**”

The high level entity used for verification is “**mayo_verify.vhd**”

The test bench reads all the data from test vector file and stores them in memory when calc=0 and WrInit pulse is received, when calc=1 the hardware module calculates the y vector and compares the y value from js implementation with resultant value and gives output as 1 if same else 0 along with output Done as high.

It was verified and working correctly for mayo1 and mayo2.