Montgomery Multiplication

Results: Architecture 2

Sadly, due to large area consumption, I was unable to test various different families of FPGAs to determine the results. For this reason, I have following the results with regard to two different word sizes for the Architecture 2 implementaton: w = 32 and w = 64.

I. Operand Size of w = 32

T_{clk} = 5.451ns
Minimum Latency = 1056*5.451ns = 5.76us = 5756.25ns
Maximum Throughput = 173721*1024 = 177.890Mbps
Area (LUTS) = 5728
Maximum Throughput/Area = 177.89Mbps/5728 = 31056.22

II. Operand Size of w = 64

T_{clk} = 6.624 ns
Minimum Latency = 1088*5.451ns = 5930.68 ns
Maximum Throughput = ((150.96*10^6)/1088)*1024 = 142.08Mbps
Area (LUTS) = 6076
Maximum Throughput/Area = 142.08Mbps/6076 = 23383.81

III. Conclusions and Comments:

Operand size for 32 bit words allows for better Maximum Throughput/Area and greater maximum throughput. I find it strange though that it will have less area than for operand sizes of 64, as having a smaller word size will lead to a larger number of processing elements dedicated to the Montgomery multiplication. I would like to investigate this strange result, but lack the time ☹