Jeremy Barthélemy

ECE 645

**Montgomery Multiplication**

*Timing Analysis: Architecture 2*

I. Latency:

With 1024 bit parameters, and 32 bit words, we will have:  
 1024 + 33 – 1 = 1056 clock cycles for a single multiplication

II. Time Between Operations:

If we disregard the SIPO/PISO logic, we can achieve a difference in time between operations of approximately 0. Due to this added logic, it will require us (operand size / word size) registers to cycle the data in, followed by an equal number of registers to convert the data out to allow for smaller usage of I/O Buffers.

III. Throughput:

Assuming no external logic, we can achieve a throughput of (183.45\*106)/1056, which is approximately 173721 multiplications per second , given TCLK = 5.451 ns for word size of 32 bits.

With 173721 multiplications per second, we are dealing with 173721\*1024 bps of data computed.