We use a 257 wide adder once which requires us only 5 clock cycle for computing a result in the worst case. It takes us around 6183 cycles to complete the montgomery multiplication and we have a rather generous 0.518 ns worst negative slack. The amount of slice LUTs is 11,889 and we are using 10,333 Flip Flops. We tried to minimize it as many as possible and further improvements would involve a more ingenous verilog code and pruning useless registers or counter. Overall, we have a rather performant montgomery multiplication with an average footprint on the board. Please see fig. 1 for understanding the FSM and the diagram (fig. 2) that became more and more complex after every iterations.

*For the TA :* I am aware that this work is below average compared to other groups but I have been for the most alone doing the software and hardware parts spending my nights trying to make this project work. Would it be possible to set up an appointment or have a discussion about this siutation. This situation is not only impacting my grades but also my own well-being. Thomas Debelle

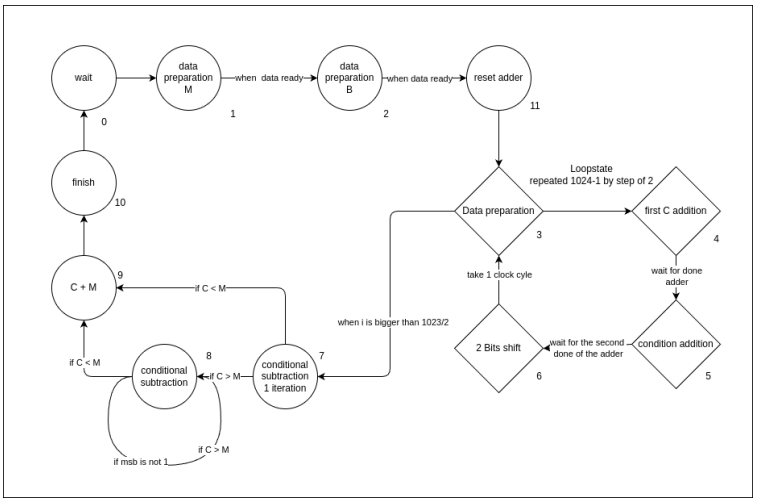


FIGURE 1 – FSM

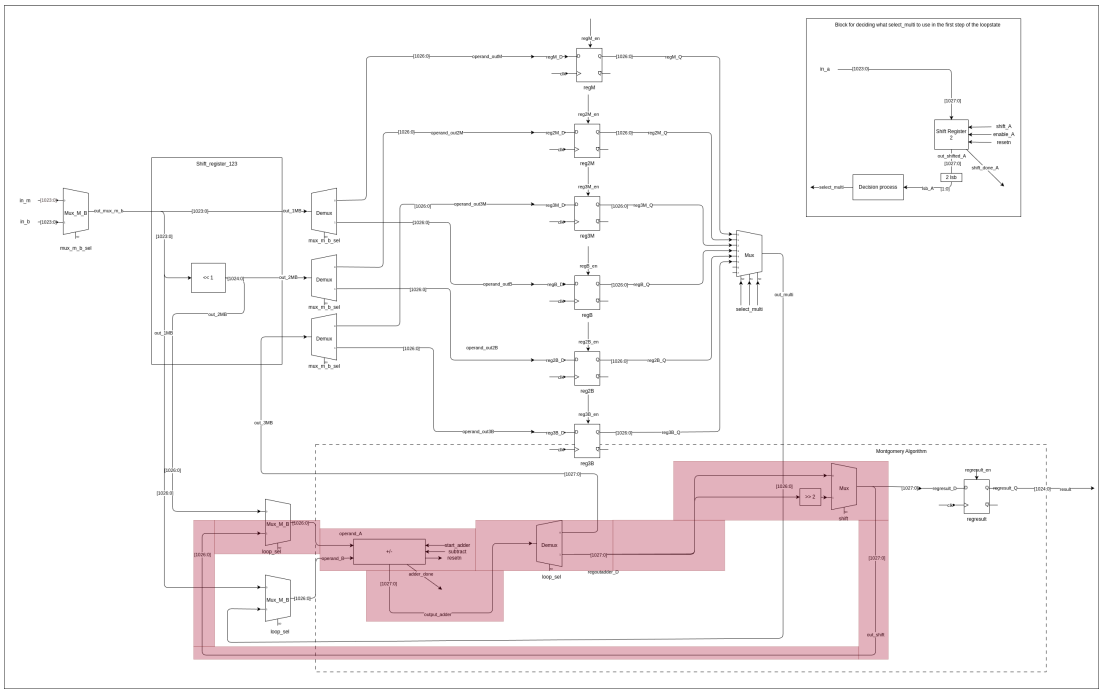

FIGURE 2 – Electronic diagram