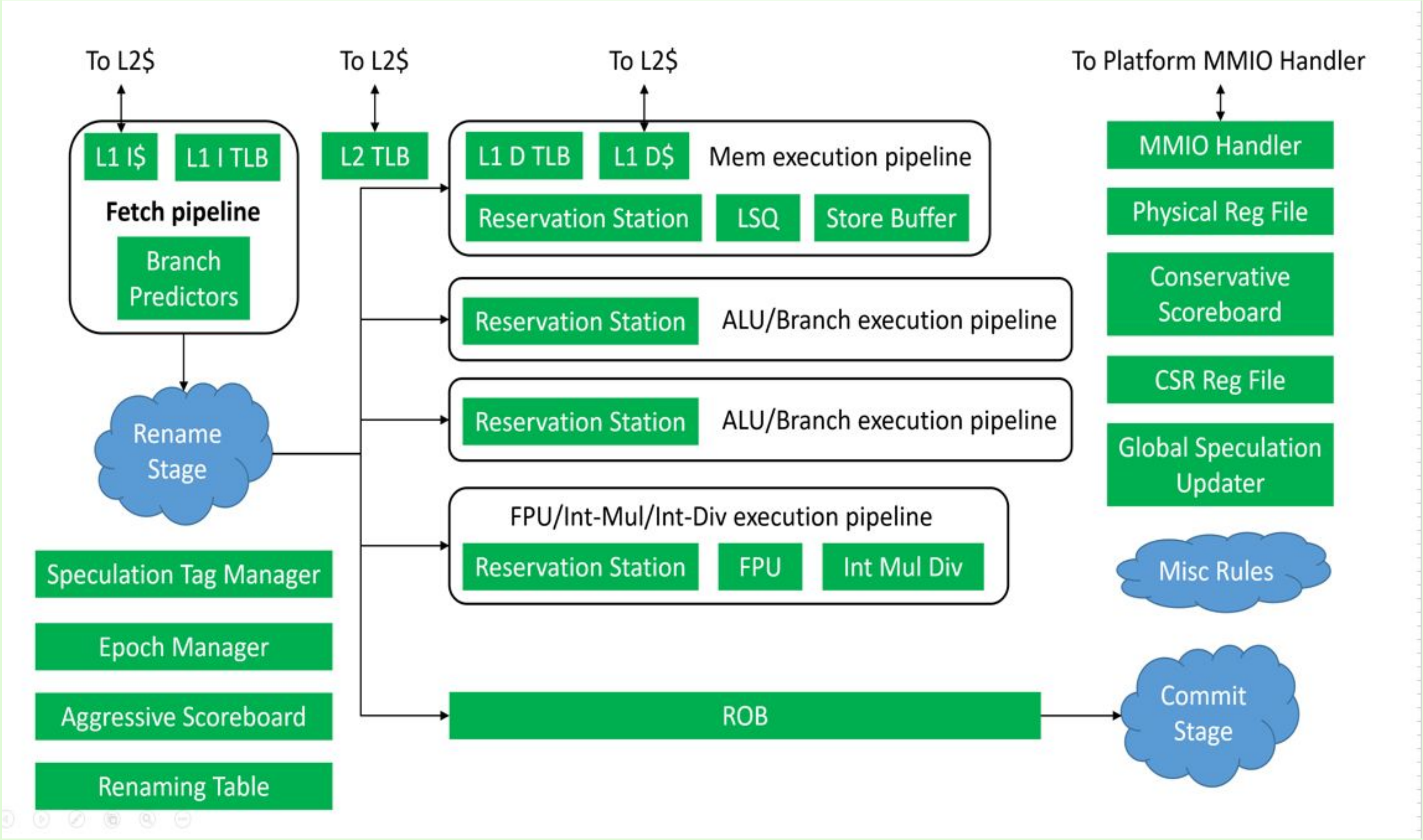
土龙 / Tulong: A Processor for Research into Secure Enclaves

Margot Bauman, Yangqiu Chen, and Zhichao Lu

Goals

-Our user story is to build a processor with DAWG security, adding mitigations against other known security vulnerabilities of secure enclaves, provides an platform for testing mitigations.

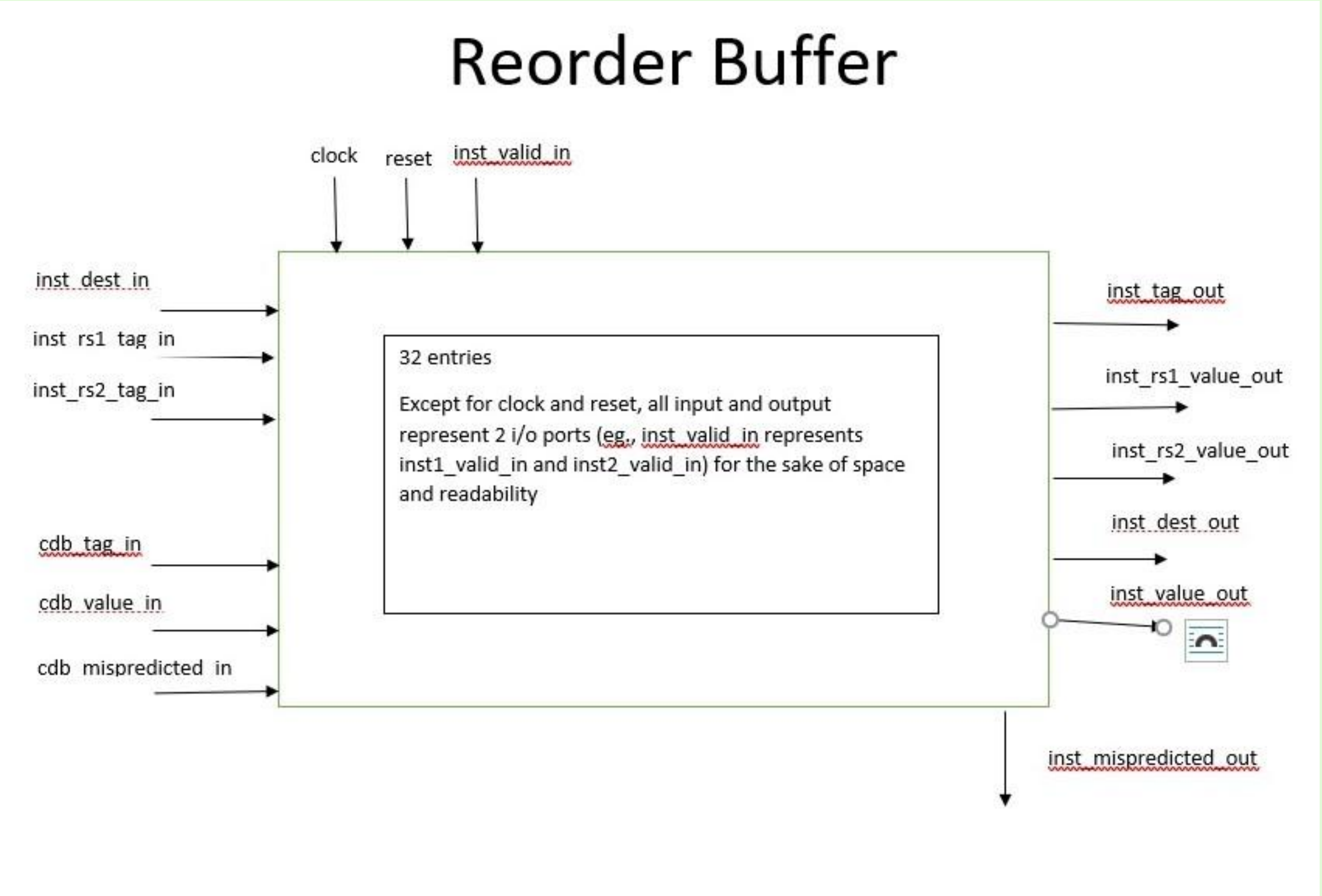
-Our MVP is MI6 processor with DAWG and other vulnerability mitigations.



https://github.com/sizhuo-zhang/RiscyOO_design_doc/blob/master/fig/core.pdf

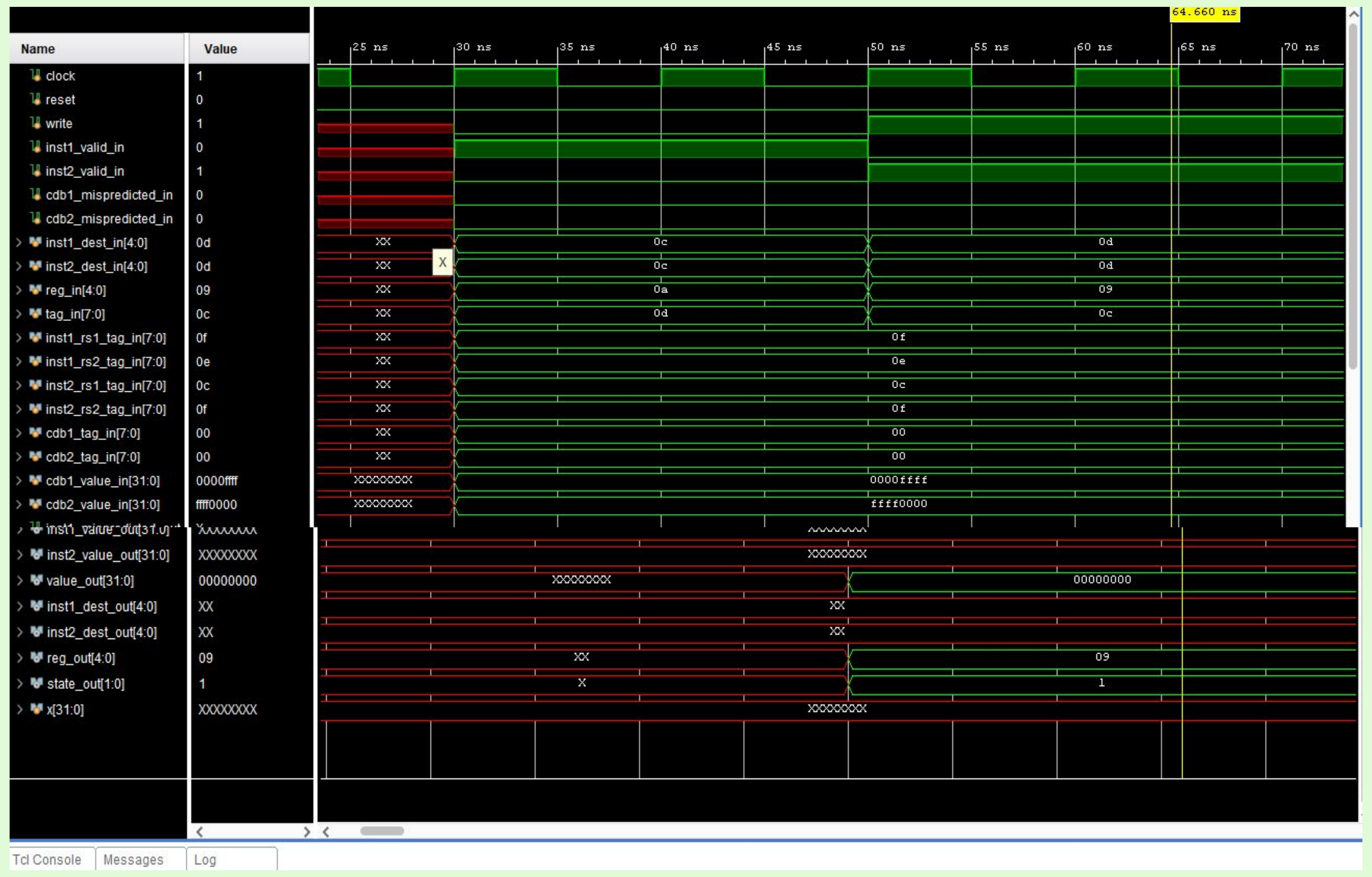
Methods

- Chose to use regular Verilog, instead of Bluespec
- Meant building OoO processor ourselves
- Got pipelined (in order) code from ASCS Lab
- Built Reorder Buffer
- Need to build Rename Buffer, Reservation Station, and other pieces as future work



32 entries

Except for clock and reset, all input and output represent 2 i/o ports (eg., inst_valid_in represents inst1_valid_in and inst2_valid_in) for the sake of space and readability



```
Name                     Value
clock                    1
reset                    0
write                    1
inst1_valid_in           0
inst2_valid_in           1
cdb1_mispredicted_in     0
cdb2_mispredicted_in     0
inst1_dest_in[4:0]       0d
inst2_dest_in[4:0]       0d
reg_in[4:0]              09
tag_in[7:0]              0c
inst1_rs1_tag_in[7:0]    0f
inst1_rs2_tag_in[7:0]    0e
inst2_rs1_tag_in[7:0]    0c
inst2_rs2_tag_in[7:0]    0f
cdb1_tag_in[7:0]         00
cdb2_tag_in[7:0]         00
cdb1_value_in[31:0]      0000ffff
cdb2_value_in[31:0]      ffff0000
inst1_value_out[31:0]    XXXXXXXX
inst2_value_out[31:0]    XXXXXXXX
value_out[31:0]          00000000
inst1_dest_out[4:0]      XX
inst2_dest_out[4:0]      XX
reg_out[4:0]             09
state_out[1:0]           1
x[31:0]                  XXXXXXXX
```

Conclusions & Lessons Learned

- Project has merit, but we made our lives very difficult
- When using open source code as a starting point, make sure all aspects of the source are open source
- Ambition is good, but realism is wise
- Ask for help, early and often

Acknowledgements

We would like to thank Prof. Michel Kinsy, Alan Ehret, Mihailo Isakov, and the rest of the ASCS Lab for their support and advice.

References can be found at:
https://github.com/MargotBauman/601-Main-Project-Secure-Enclaves/blob/master/References

Project code and notes can be found at:
https://github.com/MargotBauman/601-Main-Project-Secure-Enclaves/tree/master