**A PUF Based Trojan Evaluation for a 4 Bit Divider IP**

We have made a PUF Based evaluation for a 4 bit divider IP that demonstrates the working of the same. We made the FSM for 3 states such that each state exits and moves to the next state after 1 minute and 20 sec. so with each states moving after 1 minute 20 secs (i.e) after 4 minutes the state gets locked and there wont be any output that the 4 bit IP will produce until and unless the correct challenge response pair authentication is given to the IP. So, To say how good it is we would need to perform obfuscation metric which is given by

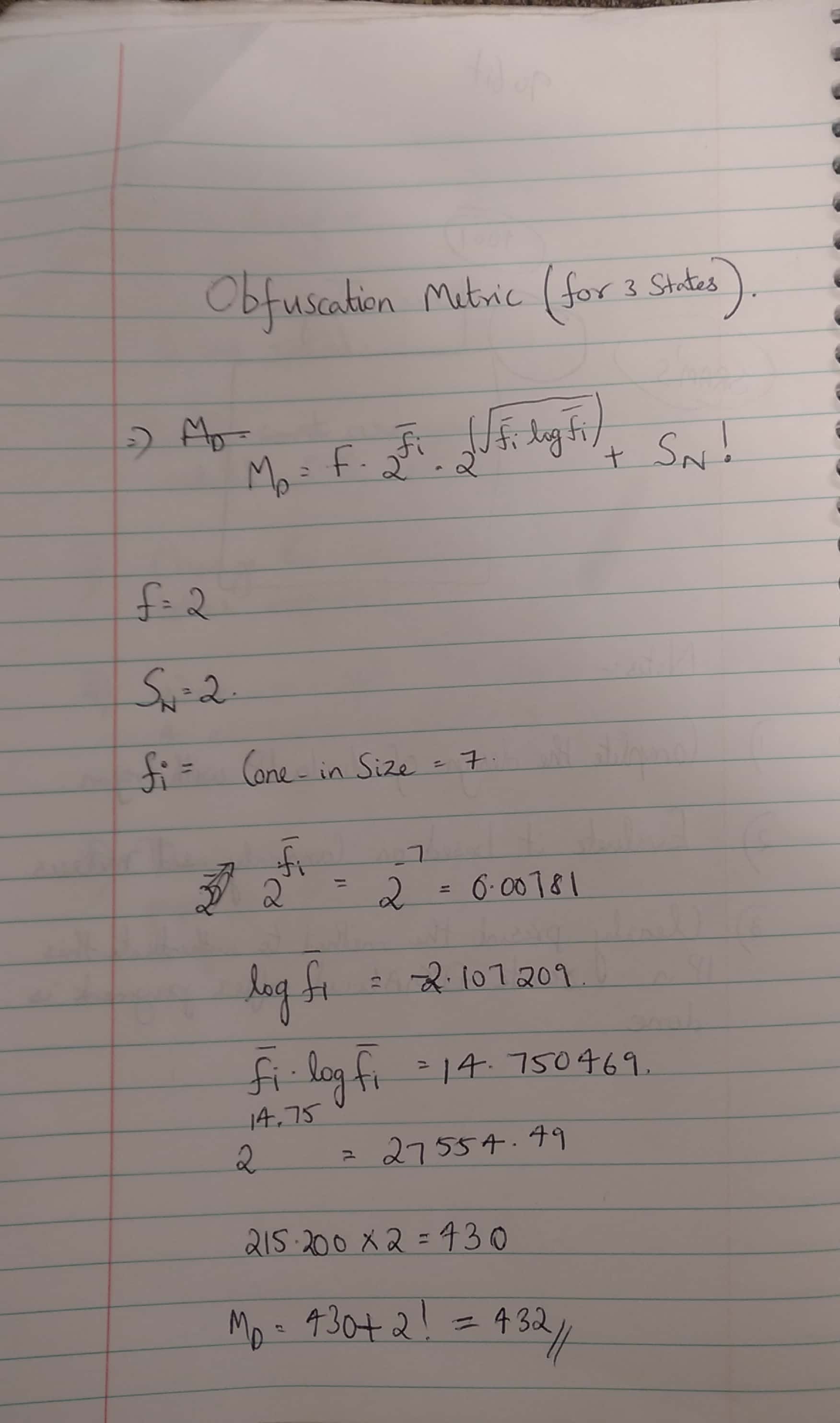
**Evaluation of Obfuscation Metric**

F- Failing nodes using formal verification

Fi – fanin cone size

Sn - Failing state elements

Obfuscation Metric derived as in the below picture:



We are getting an obfuscated metric level of 432 when considered for 3

states. If we increase the number of states then the obfuscated metric

value goes lower and it will enhance in good security strength.

The codes are uploaded in the <https://www.dropbox.com/home/PUF/siva_research/fsm%20design%20vhdl%20files> and the UCF files for Pin assignments are shown below:

Topdivid.ucf:

net "clk" LOC = "U11";

net "Remainder<0>" LOC = "F11";

net "Remainder<1>" LOC = "G11";

net "Remainder<2>" LOC = "G10";

net "done" LOC = "F9";

net "challenge<0>" LOC = "A8";

net "challenge<1>" LOC = "A9";

net "challenge<2>" LOC = "B9";

net "challenge<3>" LOC = "B10";

net "a" LOC = "E9";

net "b" LOC = "D9";

net "go" LOC = "E10";

net "Quotient<0>" LOC = "E12";

net "Quotient<1>" LOC = "D12";

net "Quotient<2>" LOC = "F8";

net "Quotient<3>" LOC = "G9";