2-bit Random Number Generator and Data Encryption

Sidhant Priyadarshi,KLE Technological University

I. Abstract

This is the implementation of 2-bit Random number generator in which initial inputs are given and output will be in random order which will be helpful for verification engineers to generate random stimulus for Unit Under Test(UUT) and also used in data encryption.In this circuit 2-bit shift registers are used and output from those two flip-flops are feedback to input of first flip-flop thus it generates random number.This is implemented using CMOS technology in Synopsys Custom Design tool.

II. Reference Circuit Details

D flip-flops are used to store the previous output and new output will be based on present input and previous output which are suitable for using in storing devices such as registers,counters,even memory can also be implemented. This is the implementation of 2-bit Random number generator in which initial inputs are given and output will be in random order which will be helpful for verification engineers to generate random stimulus for Unit Under Test(UUT)and also used in data encryption.So,here two D flip-flops are used to construct shift registers but output from those two flip-flops are feedback as input to first flip-flop and initial input is given which in turn creates random number.Here,I have contructed D-FF,INVERTER and XNOR module in CMOS Technology and further it is designed in structural model(Top-Down approach),Giving inputs like clk and clk1 which are in 180 degree of phase difference,i.e.,on the high level of clk data from first flip-flop is read and at level high of clk1 data from seconf ff is read.Now when resetn is low initial value 00 is set to ff and further it changes according to LUT(XOR) and Encrypted got as output and also 2-bit Random Number is generated.This is implemented using CMOS Technology in Synopsys Custom Design tool under the Cloud Based Analog IC Design Hackathon conducted by VSD(VLSI SYSTEM DESIGN) and IIT HYDERABAD in collaboration with Synopsys.

III. Reference Circuit

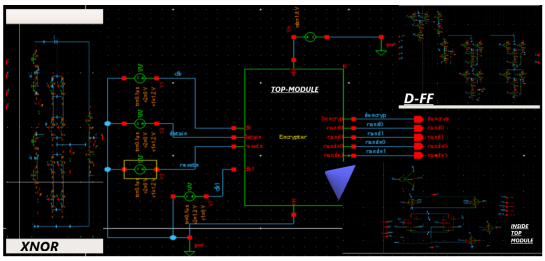

Fig. 1. Reference Circuit Diagram

IV. Reference Circuit Waveforms and Area Estimate

Area Estimated : 75 um sqr

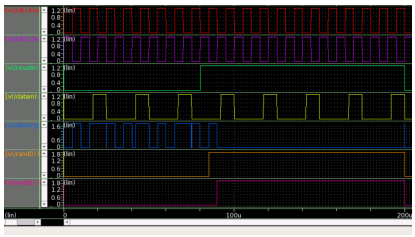

Fig. 2. Reference Circuit Waveforms

V. References

[1] Max Maxfield. Linear Feedback Shift Registers.
https://www.eetimes.com/tutorial-linear-feedback-shift-registers-lfsrs-part-3

[2]Cadence PCB Solutions. CMOS Design and circuit simulation tasks .
https://resources.pcb.cadence.com/blog/2020-cmos-vlsi-design-and-circuit-simulation-tasks