Title: 32-bit Single-Error Correcting Circuit
Submitted by: Sree Ranjani Rajendran
Abstract: This report describes the functional verification of a 32-bit single-error-correcting circuit by using COCOTB environment using Vyoma's UpTickPro framework**. This is a combinational network circuit benchmarked in 1985 International Symposium on Circuits And Systems as c499 ISCAS'85 benchmark circuit. c499_buggy circuit includes a bug, which will induce a fault in the design when a particular test pattern is applied while verification. The nature of the bug injected is discussed in the below threat model.**

Threat model:

- **A Node that propagates the fault is identified using a node detection algorithm proposed in [1].**
- **A fault will be generated at node N607.**
- **The probability of inducing a fault is 90% for a two-bit input gate.**
- **The node selected using [1] will propagate the fault towards the output without masking.**

Verification strategy:
By using the COCOTB environment using Vyoma's UpTickPro framework, a verification of the **32-bit Single-Error Correcting Circuit is done and the test vector inducing the fault is provided in the file named test_c499_buggy.py**

Bugs found
Debug information
The bug-free design is in the file, c499.v with the test verification in test_c499.py. However, the buggy design with the above-mentioned threat model is in the file. c499_buggy.v and the test case is in test_c499_buggy.py.

Ref:
[1] Rajendran, Sree Ranjani, Nirmala Devi, and M. Jayakumar. "A Node Reduction Technique for Trojan Detection and Diagnosis in IoT Hardware Devices." ***Internet of Things*****. CRC Press, 2022. 43-64.**