**Multiplierless Pseudo Random Number Generator design and Reseeding through Wireless Protocol**

**Abstract:**

This mini project is mainly focused on generating a sequence that provides randomness. This sequence is deterministic since the output sequence is completely determined by the input knows as seed. It has numerous applications in cryptography, processors, artificial intelligence, gaming and simulation.

Since multipliers required more hardware resource requirements, it heavily loads the FPGA (Field Programmable Gate Array) board and also the case of complexity,so we have approached in the way of implementing this pseudo random sequence without any multipliers. Once we generate the pseudo random number sequence, we could reseed the input information through wireless protocol.

To generate a larger random sequence, we follow the technique of continuous chaotic theory. In this theory the output generated is much sensible to the applied input. Many systems such as Lorentz, Chua, Rossler, Lu comes under chaotic theory. We decided Rossler’s system to generate our pseudo random sequence. To implement in FPGA, we use Euler’s Method to convert the differential equation to difference equation.

We are using Intel cyclone IV FPGA board for hardware and Modelsim 10.6 and Quartus prime lite 20.1 for software.

Starting with carefully analysing the mathematical equations of the multiplierless PRNG. Implement this multiplierless PRNG in FPGA using specific algorithms. Using wireless protocol, we could get back the generated PRNG and it is reseeded to get the final output. Once the implemented input for the generation of PRNG sequence and the reseeded output matches, we could validate that our work correctness and efficiency.