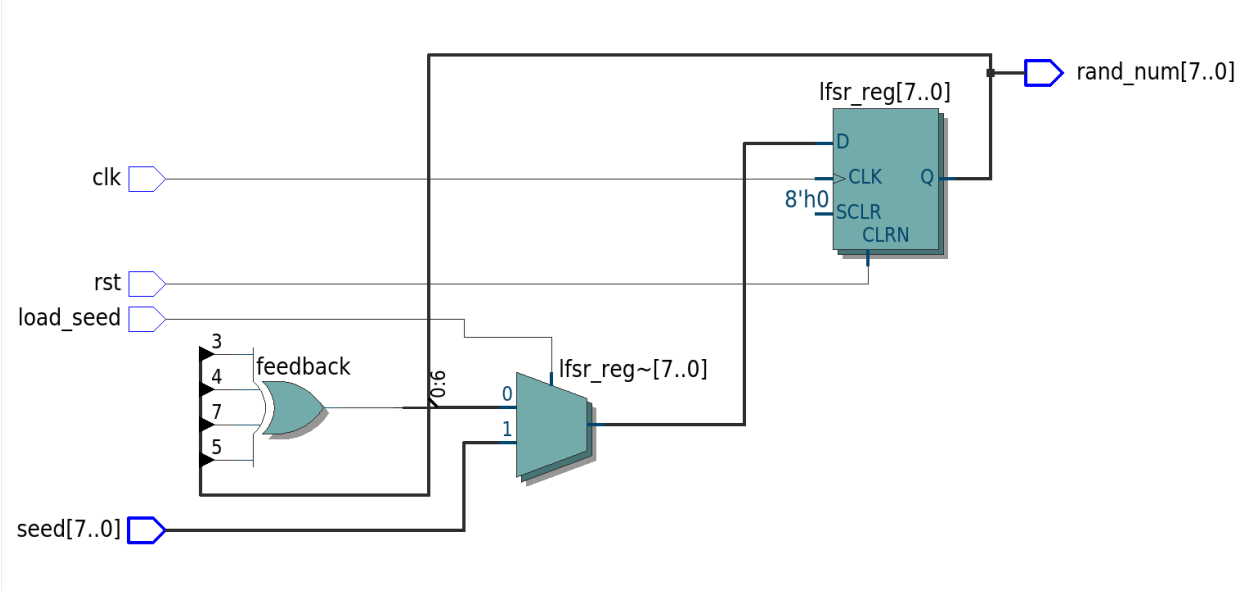
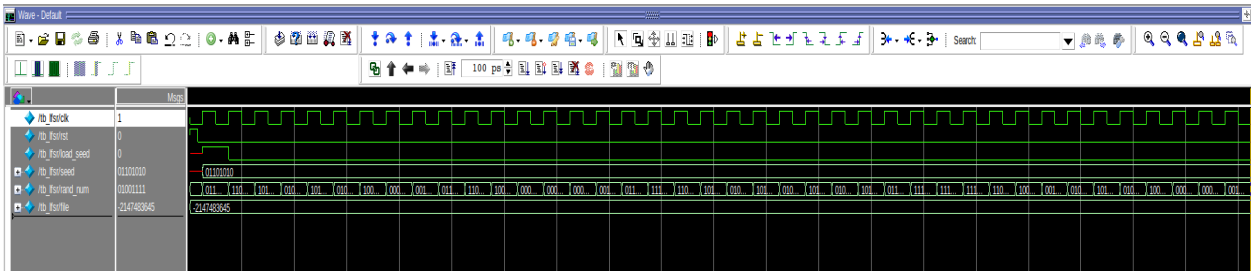
“5. Random Number Generator using LFSR”

Design:



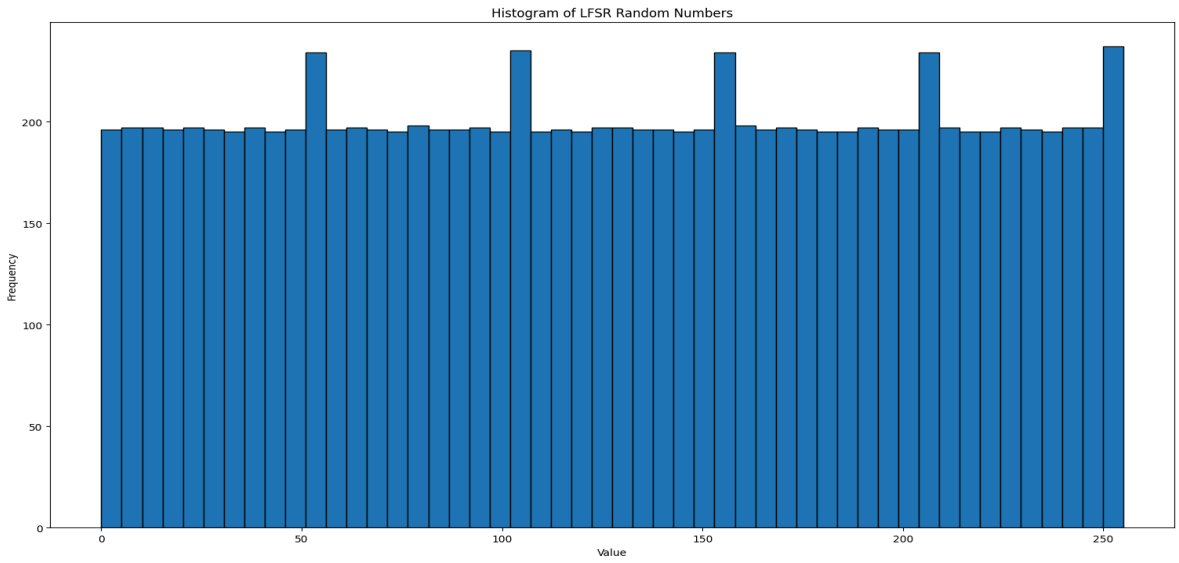
- The lfsr module implements an 8-bit linear feedback shift register to generate pseudo-random numbers.
- A seed can be loaded into the register to initialize or restart the sequence.
- On each clock edge, the register shifts left and inserts a feedback bit derived from XOR of taps (7,5,4, and 3).
- This feedback polynomial is primitive, giving a maximal length sequence before repeating (i.e. 255 unique rand numbers)
- Reset clears the register, while the current register value is continuously output as rand_num for use in designs.

Verification:



- The testbench instantiates the lfsr module and connects clock, reset, seed, and random number output.
- A clock generator with 10 ns period and reset initialization ensures proper timing.
- A fixed seed is loaded into the LFSR to begin generating pseudo-random numbers deterministically.
- 10,000 random outputs are captured using a for loop and written to a text file for later analysis.

Histogram Plot for Degree of Randomness:



- This histogram shows a near-uniform distribution of values from 0 to 255, that means indicating good randomness spread across.
- Minor variations in bar height are expected in pseudo-random sequences, but no major bias is visible.
- This confirms the LFSR taps (7,5,4, and 3) produced a maximal-length sequence with balanced output coverage.