3TB4 Lab 2 Report

Lin Fu ful10 400234794

Keyin Liang liangk10 400236736

1. We used 14 bits of XOR Fibonacci LFSR in our project that used 1, 3, 5, and 14 taps. We chose Fibonacci LFSR because it is relatively easy to implement in hardware and has a lower gate count compared to a Galois LFSR, which also has a shorter period. These taps are used because they are the positions of the most significant bit and other specific bits that have been determined to produce a maximal length pseudo-random sequence. By choosing these taps, the LFSR will generate a random sequence of 14 bits with a maximal period of 2^14 - 1, meaning it can generate all 2^14 - 1 non-zero states before repeating. This is a good choice for generating a random number in a range of 1000 to 5000, as the sequence generated by the LFSR will be uniform and evenly distributed in this range.

2. Advantages of short LFSR:

- Short LFSRs require fewer gates and less power consumption, making them more suitable for low-power applications or applications with limited hardware resources.
- Due to their simplicity, short LFSRs may be simpler to implement and verify. Also, it takes a shorter time to generate.

Disadvantages of short LFSR:

- Sequences produced are more predictable and easier to guess. So that sometimes may not generate random numbers.

Advantages of long LFSR:

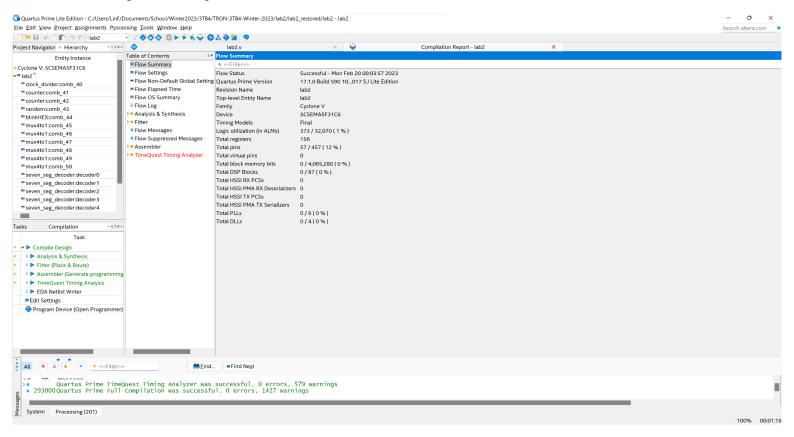
- They could create sequences that appear more random and are more difficult to anticipate, making them better suited for cryptographic applications.
- They are more suitable for applications that require longer sequences.

Disadvantages of long LFSR:

- Long LFSRs may need more gates and use more power and time, which makes them less appropriate for low-power applications with limited hardware resources.
- They could be trickier to develop and test, and hence more likely to have design problems.

3.

Complication Report:



Total number of logic elements used by your circuit: 373

Total number of registers: 156 Total number of pins: 57/457

The maximum number of logic elements that can fit on the FPGA that you used: 32070