2020

Implementation of Pseudo-Random Number Generator Using LFSR

Touheda Khanom
CUNY New York City College of Technology

Fahmeda Khanom
CUNY New York City College of Technology

Implementation of Pseudo-Random Number Generator Using LFSR

Fahmeda Khanom & Touheda Khanom
Mentor: Yu Wang
New York City College of Technology, Computer Engineering Technology, Honors Scholars Research Program

Linear Feedback Shift Registers (LFSR) play a vital role to provide cybersecurity for the data communication system. LFSR is a shift register where the input is linear of its previous states. The most important application of LFSR is the device's ability to generate a pseudo-random sequence of values that are used in encryption and decryption to secure personal data. Moreover, LFSR is used in Cyclic Redundancy Check Calculations (CRC) which can help to detect errors and corruption in data communications as LFSR feedback values can be modified. The main objective of the research is to generate the pseudo-random sequence of values in 3-bit, 4-bit, and 8-bit using the multiple registers with XOR as different taps selection. In the research, we used D(Data) flip flops and XOR alternative taps to identify the difference in the values for different arrangements in circuit diagrams using the software Quartus. After the simulation, we test the circuit on the Field Programmable Gate Array (FPGA) board to check the generated binary random number displaying the LED "on" or in "off" state.

INTRODUCTION

Rapid technology advancement became a prime concern when Cybersecurity and the privacy of human data became vulnerable to hackers. Engineers are working hard to build strong security to prevent hackers from damaging hardware, software, or electronic data. Generating pseudo-random sequences of values using Linear Feedback Shift Register can help to build strong security to avoid unauthorized access to private information. LFSR is also used in cryptography to encrypt and decrypt electronic data which helps to secure all our ATM cards, computer passwords, and electronic commerce [1]. Moreover, Cyclic-Redundancy-Check(CRC) is used to detect error or corruption during signal data transmission which are possible to easily implement in hardware using LFSR. The sequence of values stored in the LFSR is known as checksum and receivers check out the internal checksum generation with the checksum in the transmitter to figure out the real problems[3]. If there is no fault or corruption the receiver check produces all zeros. XOR plays a vital role because with the help of alternative tap selection we can get different random values. The main purpose of the research is to use LFSR to generate pseudo-random values with the help of shift registers and XOR alternative tap selections.

METHODS

- In LFSR each D flip flop represents a single bit of data
- We built 3-bit, 4-bit, and 8-bit shift register block designs using intel Quartus ii and did functional analysis.
- In our designs, all flip flops share the common clock input which is labeled as CLK
- CLK input is known as edge-triggered because the circuit activates when clock goes from low to high as we are using positive edge of the clock signal
- We used 2 different taps at bit 0 and 7 bit for figure 1 and at bit 3 and bit 7 for figure 2 and tested how alternative tap selection provides us with different pseudo-random values on figure 3 and figure 4.
- We group our output in vector based on waveform simulation data to get a clear observation of the sequence in decimal format of pseudo-random numbers generated based on the circuit
- We work on the FPGA board and test each block design to observe the binary on and off state at binary display

BLOCK DESIGNS

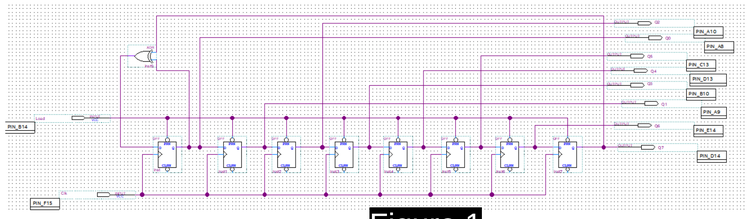

Figure 1

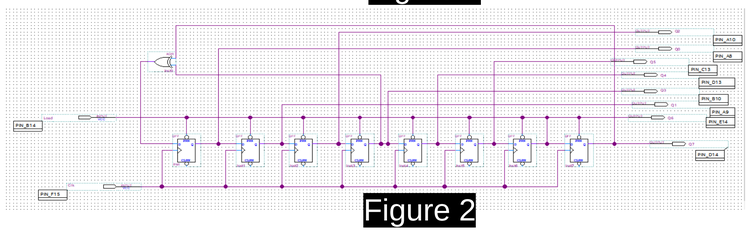

Figure 2

TIMING ANALYSIS / WAVEFORM

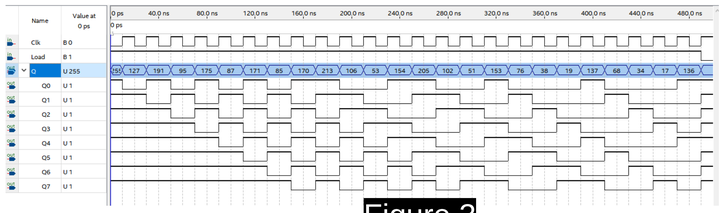

Figure 3

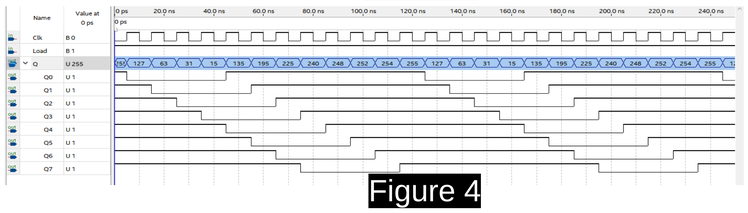

Figure 4

OUTPUT FROM FPGA EDUCATIONAL BOARD

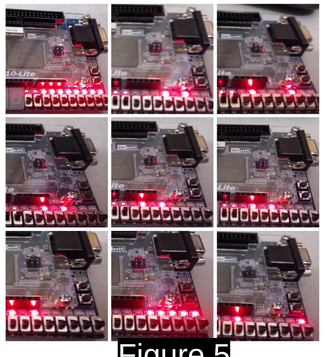

Figure 5

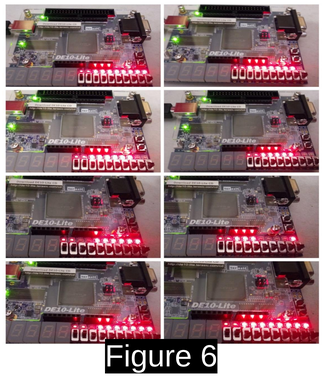

Figure 6

RESULTS

From the experiment of different taps location applied to 8-bit group of registers generates pseudo-random outputs. When the load is on the high state and the clock pulse changes from low to high, we see the output values change. Moreover, we noticed that after a certain clock pulse we get repeated values on the outputs. 8-bit has 255 lengths of loops using 2^n-1 where n represents the number of registers used in the circuit. Similarly for 4-bit we have 15 lengths of loops that have 15 random values before the values start repeating[2]. If the tap selection is different, we get different sequence of numbers.

Table 1

Block Designs #1 Decimal Random Values	Block Designs #2 Decimal Random Values
255	255
127	127
191	63
95	31
175	15
87	135
171	195
85	225
170	240

CONCLUSION & FUTURE WORK

Based on our research, we can conclude that LFSR serves multiple important purposes in real life applications. LFSR makes it easier for cybersecurity, CRC, cryptography and pseudo random generators. Hardware and software can be used to work on random number generators. For future work, we would like to work on the software skills and will use Verilog code. We would deeply work on CRC and use different approaches like one-to-many implementation and more than two taps alternative using XOR to get more random values.

ACKNOWLEDGMENTS

Honors Research Scholars Program
Special Thanks to Professor Yu Wang

REFERENCES

[1]
"Cryptography | Crypto Wiki | Fandom." https://cryptography.fandom.com/wiki/Cryptography (accessed Nov. 17, 2020)
[2]
M. Maxfield, "EETimes - Tutorial: Linear Feedback Shift Registers (LFSRs) - Part 1 -," *EETimes*, Dec. 20, 2006. https://www.eetimes.com/tutorial-linear-feedback-shift-registers-lfsrs-part-1/ (accessed Nov. 17, 2020).
[3]
Felsa Mary Fidus, Lalmohan K. S, Ambika Sekhar, and Sree Buddha College of Engineering, "Design and Implementation of a Secure Stream Cipher for Cryptographic Applications," *IJERT*, vol. V4, no. 07, p. IJERTV4IS070422, Jul. 2015, doi: 10.17577/IJERTV4IS070422.