

Reconfigurable linear feedback shift register for wireless communication and coding

Aakanksha Devrari, Adesh Kumar

Department of Electrical and Electronics Engineering, School of Engineering, University of Petroleum and Energy Studies, Dehradun, India

Article Info

Article history:

Received Aug 23, 2022

Revised Oct 15, 2022

Accepted Dec 10, 2022

Keywords:

Gold sequence

Linear feedback shift register

VHDL

Wireless communication

Xilinx simulation

ABSTRACT

Linear feedback shift register (LFSR) is the basic building block of the communication system used in different coding, error detection and correction codes, such as gold, low-density parity check (LDPC), polar, and turbo codes. There are simple shift register-based n-bit counters with a few XOR gates that behave pseudo-randomly. The LFSR is used in chip hardware for high-speed operations, error control, and the generation of pseudo-random numbers. The hardware chip design and performance estimation of the LFSR is the problem for specific communication system. The motivation of the work is to generate the Gold code sequence by the integration of two LFSR. The article proposes the hardware chip design and simulation of two 5-bit LFSR modules used for the gold sequence generator applicable for the communication systems. The novelty of the work is that the design is scalable and can be extended based on the requirements of the systems which is synthesized and experimentally verified on the Zynq-7000 field programmable gate array (FPGA) board. The concept of this design is programmable and can be extended to n-bit based on the applications. The work is supported, and formulated using very high speed integrated circuit hardware description language (VHDL) programming in Xilinx ISE 14.7 software.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Adesh Kumar

Department of Electrical and Electronics Engineering, School of Engineering

University of Petroleum and Energy Studies

Via Prem Nagar, Bidholi Campus Dehradun, Pin-248007, India

Email: adeshmanav@gmail.com

1. INTRODUCTION

The linear feedback shift register (LFSR) is essentially a shift register that moves data from one register to the next with each clock signal [1]. Linear feedback is formed by XORing some bits of the shift register to drive the input values of the LFSR. The selected bits in the preceding states influence the input bits and are referred to as taps. The feedback loop is formed by XORing a series of such taps that are dependent on the feedback polynomial. A lot of work is carried out in the direction to make the reconfigurable LFSR which can be future utilized for Gold code, different communication systems, and switching applications. Reconfigurability and speed are the essential properties to make the system suitable for coding and communication. Reconfigurability refers to re-programmability that provides the platform to the reprogrammable generators with significant capabilities to control LFSR operations at the same speed [2]. The extraordinary advancements in optical components and devices in current years have resulted in major efforts in implementing optical signal processing methods. LFSR played an important role in classical electronics, such as circuits that generate encryption and decryption, pseudorandom binary sequence (PRBS),

and a bit error rate measuring system [3], [4]. Optical LFSRs, which have the advantage of speed, are predicted to provide benefits in similar types of applications. Optical fiber shift registers [5] with the integration of XOR gate [6], [7] and semiconductor optical amplifier (SOA), having low transferring energies and advanced switching speeds (>40 Gb/s) proved to achieve this goal. The enormous length of optical shift registers limits the usefulness of optical LFSRs because of the complexity of programming while generating the regulated PRBSs.

In the scheme of grouping numerous concurrent transmissions for a multichannel network using the same physical link, the bandwidth of optical fiber can be utilized properly. In a network setting, this goal can be met by employing multiple access techniques, like code division multiple access (CDMA) and frequency division multiple access (FDMA) probably in conjunction with logical communication techniques. CDMA [8] has been used to address multiple users in a rational optical network, while [9] proved the practical viability of a spreading dispreading [10] electro-optic modulator. Gaussian approximation was proposed for the random variable in the deficiency of noise to solve the interferer effect and the performance of a CDMA system with Gold sequences was evaluated in [11]. The flaws in both assumptions have been thoroughly examined in recent papers for optical and wireless communication. In the disparity to the particulars of electro-optical conversion, it is an essentially random behavior that can be experienced in the presence of shot noise. The non-existence of noise provides error-free transmission in the case of a small population of interferers. The feedback parameters are acquired by a matrix transformation from the control LFSR output. The disparity between the controller and controlled FSR in the design provides the period benefits over the suggested approach of varying feedback shift registers [12]. The ability to use arbitrary feedback functions for the controlled FSR and an arbitrary controller additionally increases our design's degree of freedom. Variable feedback has been implemented earlier. The switch-controlled feedback sequentially moves a single There is no change in speed between the control and the reconfigured FSR, and the reconfigured FSR is confined to an LFSR. As a result, complexity is highly promising for a simple method.

Decimation has been used to create variable characteristic polynomials in a variety of ways, the simplest of which is the stop-and-go generator, in which the output of one LFSR controls the clock of another. For example, when the output of a controlling LFSR is '1', an LFSR may step through one cycle of its clock, but not when the output is '0'. The study examined several clock-controlled LFSR designs "including cascades of LFSRs driven by the same clock source. Due to the necessity that each LFSR has several gates, this requirement may be a challenge for optical logic implementation due to gate count constraints. Another type of clock-controlled sequence is the LFSR-based shrinking generator but these generators are insecure when the feedback functions contain a small number of nonzero terms. However, optical memory is built by circulating bits rapidly through fiber and has few points of access for users. The feedback function will utilize the majority of bits in the register, i.e. the optical memory, at any one time. As a result, the feedback function will contain a high proportion of zeros, which is precisely the limitation one wants to avoid in the taps and the feedback function. The speed differential concept was discussed between two FSR [13], in which the outputs of two LFSR operating at different speeds are combined nonlinearly but the speed difference between the two sequences 'm' is not reconfigured. This fiber has previously been demonstrated to be insecure. The approach is different from the reconfigurable FSR in the absence of a sequence-controlled FSR.

The gold sequence generator is using the two identical input sequences of LFSR output which are XORed. The two input sequences should have the same phase connection until all of the additions are made. A completely different gold sequence occurs from even a slight phase modification in one of the input sequences. This behavior is depicted in Figure 1.

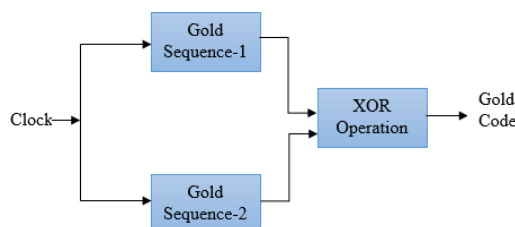


Figure 1. LFSR and Gold code output

LFSRs are frequently used in stream ciphers to produce pseudorandom sequences which are further used in data security encryption and decryption. The novelty of the study is that it offers a platform for chip

designers and researchers to replicate the capability of scalable LFSR and gold sequence generator on high-end field programmable gate array (FPGA), ensuring the integration of the same chip for the next generation of communication systems, such as 5G and 6G. The data size of the LFSR used in the simulation is 5-bit. Therefore, the datapath size is 5-bit as one-bit storage is applicable to one flip-flop. The objective of the work is to perform the simulation for the same functionality.

The organization of the manuscript is as: the section 2 presents the proposed method of LFSR in serial and parallel execution levels. Section 3 presents the implementation architecture of the 5-bit sequence and methodology. Section 4 presents the results and discussions part with the possible simulation test inputs and FPGA board experimental verification followed by conclusions in section 5.

2. PROPOSED ALGORITHM

The serial implementation of a linear feedback shift register [14], [15] is depicted in Figure 2. It is clear from the system behavior that the serial architecture has two drawbacks: first, every clock causes the entire structure to become time-locked, and second, only one information bit is produced. It is possible to overcome these issues by utilizing a parallel design in which one or two cells are synchronized at the same time. LFSR circuit has a large number of connections between its structure and the XOR tree because all the taps [16] are connected to the flip-flops (FFs) individually for the circuit to function properly.

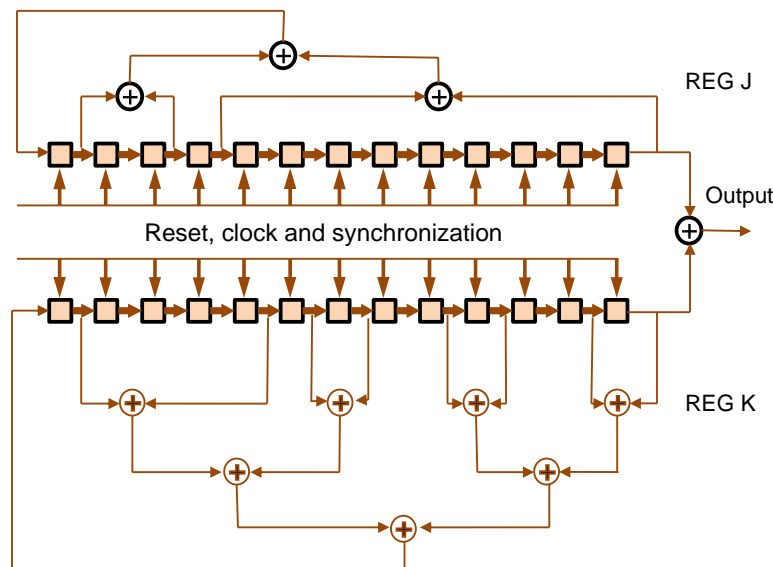


Figure 2. The basic principle of serial LFSR

Figure 3 depicts an example of parallel LFSR architecture. Individual cells in the register remain unchanged in this configuration unless updated once in every 'N' clock cycle. Taps generally move in the direction following the preceding cell with each clock cycle, but the bits contained within the memory elements remain unchanged. As a result, the tap which was previously connected to cell number 6 has been moved to cell number 5, and the tap previously connected to cell number 5 has been moved to cell number 4, while the tap earlier connected to cell number 1 (initial cell) has been moved to the cell number 7.

The tap initially connected to cell number 1 (initial cell) has been reconnected to cell number 7 (last cell). It is similar to the impact of bits being redistributed to the next higher cell [17] in traditional architecture. The control unit [18] instructs the switches to update every cell in sequential order with the values, which is obtained from the XOR tree on each clock cycle. The array memory elements only transition once as a result, and the remaining FFs stay static and use no power. While this architecture consumes more hardware than traditional architecture, it switches less circuitry per clock cycle, resulting in lower power dissipation of the system. A large number of components are required in this architecture, as each XOR tree tap must first scan the entire array and it should be connected to each memory cell, totaling N (cells number) \times M switches (taps number). Besides this, the total number of components can be reduced to $(N+M)$. Only one transistor is required to physically implement each switch.

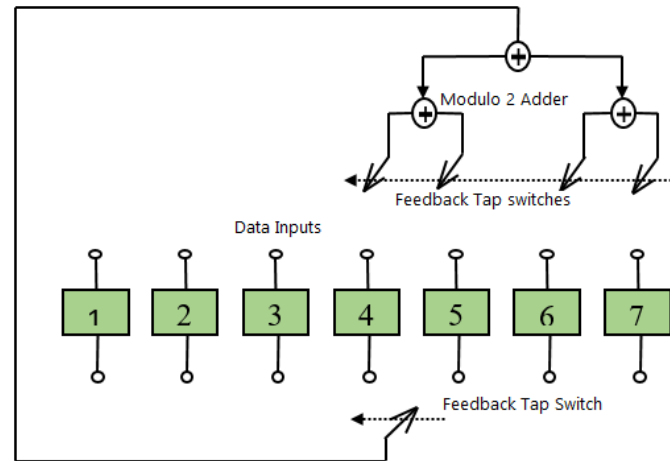


Figure 3. Basic principle of the parallel LFSR

3. METHOD

Gold codes [12] are created by XORing two maximum-length sequences having the same length. These sequences are added to the computer chip using synchronous clocking. The difference in the phase position of two generated m-sequences results in the generation of a fresh sequence. A Gold code is produced using specially chosen m-sequences, also known as preferred m-sequences. A LFSR has two $(2n-1)$ states [19], [20], where 'n' is the LFSR's register count. At the start end of each clock edge, the contents of the shift registers are moved one position to the right [21]. Preset registers or register taps are used in conjunction with the register to provide feedback. These will use an XNOR or XOR gate to provide feedback to the leftmost register. When employing XOR feedback, it is forbidden to have a value of all 1s or all 0s because doing so would result in the counter becoming trapped in this state. LFSRs can be used to convert narrowband signals into simulated noise. LFSRs are used to convert a narrowband signal to a wideband signal, which generates pseudo-noise in the process. The feedback function of an LFSR is one of the device's two fundamental components, the other being the shift register. Shift registers are primarily used to relocate register contents into neighboring positions inside a register, or out of the register if the position is at the end of the register. The area will remain empty unless fresh content is provided to the register's other end.

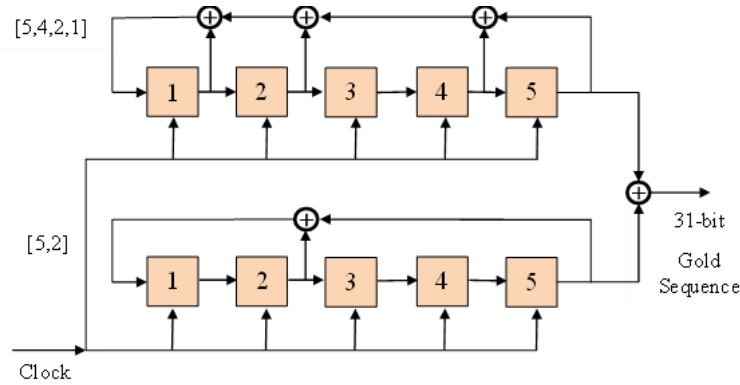
In Gold code generators, LFSRs are the most fundamental functional block. When 'N' registers are used in the LFSR, it cycles through $(2n-1)$ states, which is a prime number. As shown in the diagram, each clock cycle causes the contents of the registers to be moved from one position to the right. The rightmost register is produced by XORing the leftmost register with feedback from predetermined registers or taps. When designing LFSRs, the number of taps in each feedback route, as well as the number of steps in the shift register, must be taken into account. Another variable is the shift register stage or the location of each tap. To function efficiently, a class of spreading codes in a multiple-access system must have the minimum possible value of mutual interference. The technique uses the Gold subclass of PN sequences [21]. These are chosen such that the cross-correlation scores between the codes in a specific set are uniform and bounded across the entire set. The addition of the code sequences occurs one at a time using synchronous clocking. The length of the generated codes is equal to the length of the two m-sequences added together. One advantage of using Gold codes is their ability to generate a large number of codes. Consider the following case:

$g_1(X)$ and $g_2(X)$ are assumed to be the desired primitive polynomial pair of degree 'n', in which the respective shift registers produce a maximal length sequence of the period $2(n-1)$, whose cross-correlation function is less or equal to 1.

$$2^{\frac{n+1}{2}} + 1 \text{ for } n \text{ is odd} \quad (1)$$

$$2^{(n+2)/2} + 1 \text{ for } n \text{ is even} \quad (2)$$

If the preceding condition is met, $g_2(X)$ will produce $2(n+1)$ distinct sequences, each having a duration of $2(n-1)$. The process of making a Gold set is featured in the illustration in Figure 4 that follows the Gold code sequence generator with shift register of length $m=5$.

Figure 4. Gold code sequence generator with shift register of length $m=5$

It is proposed to use linear feedback shift to reduce the length of a sequence to its shortest possible length [21], [22]. The length of the register is $m=5$. The feedback taps are chosen from the sets (5, 2) and (5, 4, 2, 1) as shown in Table 1. Table 1 illustrates the evolution of maximal length sequences, where the generator returns to its initial state after 31 iterations, assuming the initial state is 10000.

Table 1. The maximum length sequence of LFSR with 5-bit input data 10000

State	LFSR-1 Tap (5, 2)	Output LFSR-1	LFSR-2 Tap (5, 4, 2, 1)	Output LFSR-2	Gold sequence
0	10000	0	10000	0	0
1	01000	0	01000	0	0
2	00100	0	00100	0	0
3	00010	0	00010	0	0
4	00001	1	00001	1	0
5	10100	0	11101	1	1
6	01010	0	10011	1	1
7	00101	1	10100	0	1
8	10110	0	01010	0	0
9	01011	1	00101	1	0
10	10001	1	11111	1	0
11	11100	0	10010	0	0
12	01110	0	01001	1	1
13	00111	1	11001	1	0
14	10111	1	10001	1	0
15	11111	1	10101	1	0
16	11011	1	10111	1	0
17	11001	1	10110	0	1
18	11000	0	01011	1	1
19	01100	0	11000	0	0
20	00110	0	01100	0	0
21	00011	1	00110	0	1
22	10101	1	00011	1	0
23	11110	0	11100	0	0
24	01111	1	01110	0	1
25	10011	1	00111	1	0
26	11101	1	11110	0	1
27	11010	0	01111	1	1
28	01101	1	11010	0	1
29	10010	0	01101	1	1
30	01001	1	11011	1	0
31	10000	0	10000	0	0

The design technology of the work is as follows. The chip functionality follows the steps of the chip design, and simulation modeling. The Verilog hardware description language (VHDL) programming is used to design the LFSR-1 chip that accepts the 5-bit input stream with the tap sequence (5, 2). After that, the LFSR-2 chip is designed that also accepts the 5-bit input stream with the tap sequence (5, 4, 2, 1). The waveform simulation is carried out for both the LFSRs in which the test cases are verified. The real-time verification is done on the FPGA board to check the feasibility of the design. The methodology for the same is given in Figure 5.

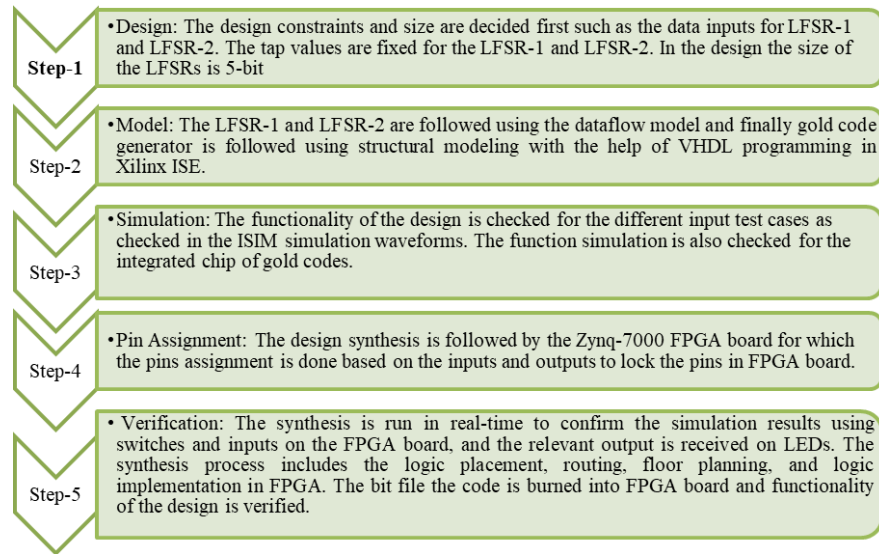


Figure 5. Methodology

4. RESULTS AND DISCUSSIONS

The simulation of LFSR-1, LFSR-2, and the Gold code generator is done in Xilinx ISE 14.7. The register transfer level (RTL) of the same module is depicted in Figure 6, which presents the inputs and outputs pins used in the design. The details for the pins utilized are listed in Table 2. In the design, the 5-bit input sequence is processed and controlled using the tap sequence. The tap bit positions are (5, 2) and (5, 4, 2, 1) for LFSR-1 and LFSR-2 respectively.

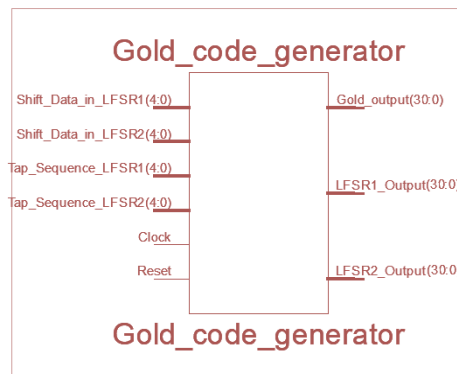


Figure 6. RTL of Gold code generator with 5-bit input

Table 2. Pins details of the LFSR and Gold code generator

Pins	Function
Shift_data_in_LFSR1(4:0)	It presents the 5-bit input to the LFSR-1 module given as the sequence-1 input
Shift_data_in_LFSR2(4:0)	It presents the 5-bit input to the LFSR-2 module given as the sequence-2 input
Tap_Sequence_LFSR1(4:0)	The taps are the bit positions that have an impact on the subsequent state. It presents the bit position for feedback, and the output bit is sent back into the leftmost bit after each tap is successively XORed with it. It is the 5-bit input given to the LFSR-1 module.
Tap_Sequence_LFSR2(4:0)	It presents the bit position for feedback for the LFSR-2 module, in which the output bit is sent back into the leftmost bit after each tap is successively XORed.
Clock (1-bit)	Click is the input given to LFSR-1 and LFSR-2 to work on the active edge of the clock signal. In the design, 50% duty cycle is used.
Reset (1-bit)	Presents the input applied for the rest of the LFSR contents as zero.
LFSR_out1(30:0)	The output of the LFSR-1 module is derived as the 31-bit simulated output.
LFSR_out2(30:0)	The output of the LFSR-2 module is derived as the 31-bit simulated output.
Gold_out(30:0)	The output of the gold sequence module, which is derived from the 31-bit XORed output

The simulation of the LFSR-1 is shown in Figure 7, the simulation of LFSR-2 is shown in Figure 8, and the Gold code simulation output waveform is shown with the help of Figure 9. The simulation waveform is taken from the Xilinx ISIM simulator [23], [24]. The simulation provides the hardware and timing reports for further analysis [25]. The test inputs and outputs help to understand the functionality of design.

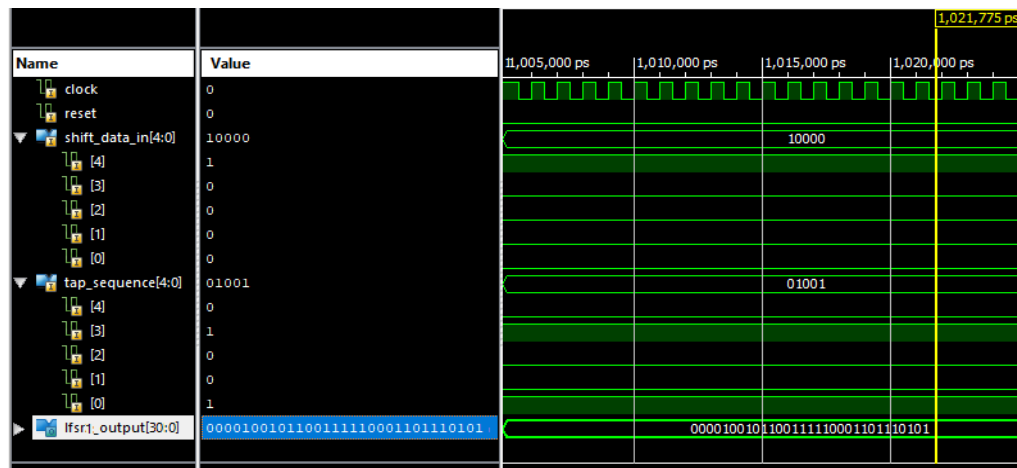


Figure 7. The output of LFSR-1 with tap (5, 2)

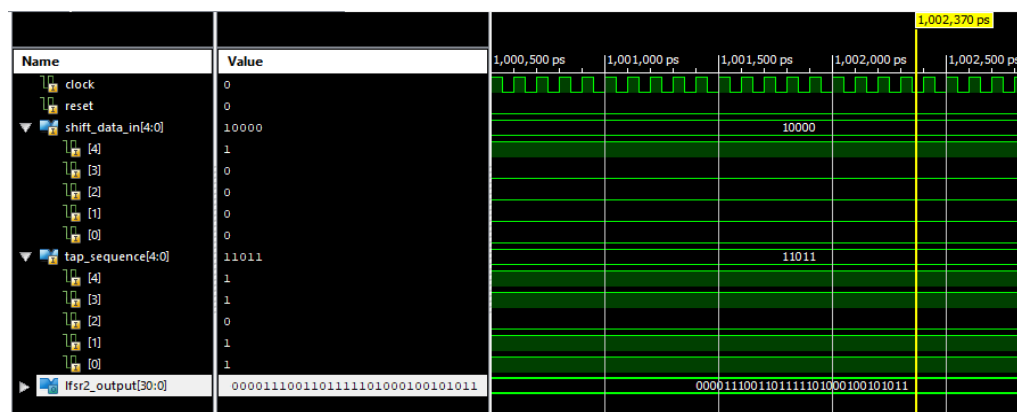


Figure 8. The output of LFSR-2 with tap (5, 4, 2, 1)

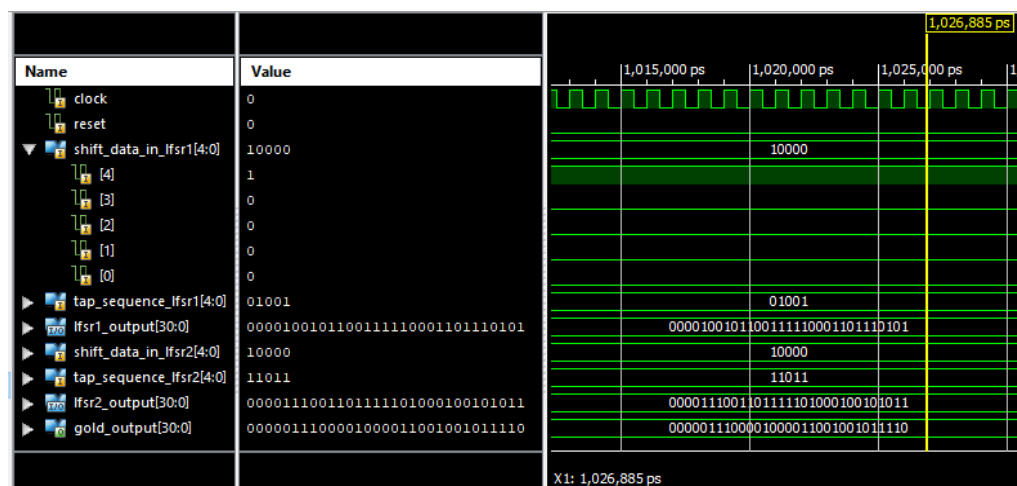


Figure 9. Gold sequence output

Test input for LFSR-1: sequence input, Shift_data_in_LFSR1 (4:0)="10000", Tap inputs [5, 2] as Tap Sequence_LFSR1 (4:0)="01001", the output of LFSR-1(30:0)=000 0100 1011 0011 1110 0011 0111 0101 (in binary)=04B3E375 (hexadecimal). Test input for LFSR-2: sequence input, Shift_data_in_LFSR2 (4:0)="10000", Tap inputs [5 4 2 1] as Tap Sequence_LFSR2 (4:0)="11011", the output of LFSR-1(30:0)="000 0111 0011 0111 1101 0001 0010 1011" (in binary)=04B3E375 (hexadecimal). The output of the gold sequence is Gold_out (30:0)="000 0011 1000 0100 0011 0010 0101 1110" (in binary)=0384325E (hexadecimal).

Figure 10 shows the simulation data verified in the real-time environment for that the FPGA kit is configured with the pin assignment as depicted in Figure 10(a) and Figure 10(b). The bit file is burned into FPGA as shown in Figure 11. The FPGA synthesis comprise the steps of technology mapping, pins mapping, logic placement, and routing in the targeted device. The switches are applied inputs and "01001", and "11011" for both cases respectively, and the corresponding output is verified on LED output byte by a byte which is "00000100 10110011 11100011 01110101" and "0000 0111 00110111 11010001 00101011" respectively. The verified gold output on the kit is "00000011 10000100 00110010 01011110".

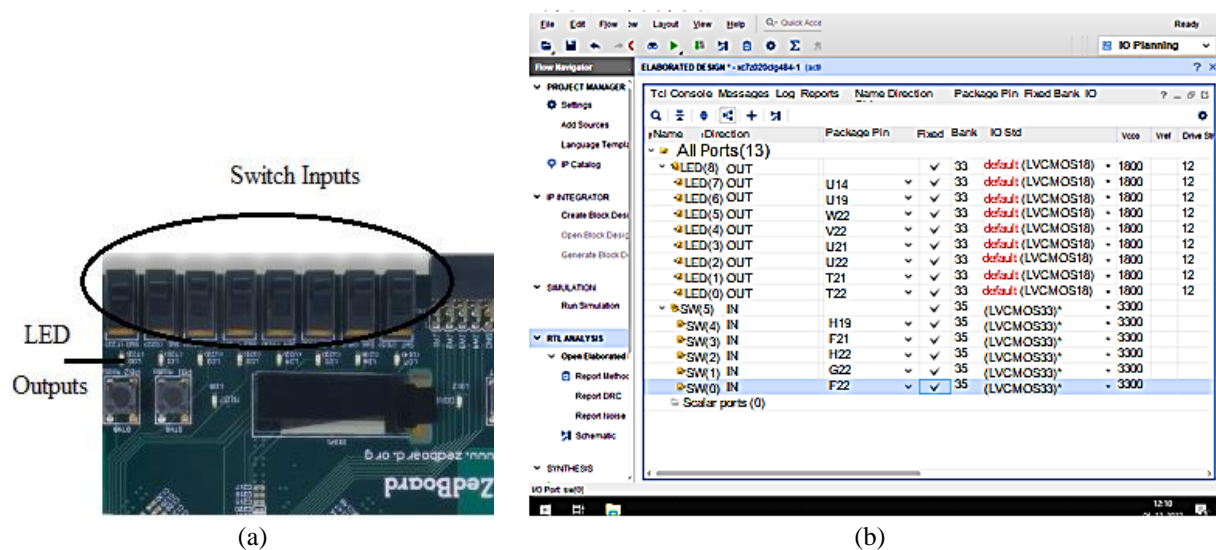


Figure 10. Verification of the logic on FPGA (a) switch as inputs and LEDs as outputs and (b) pin assignment



Figure 11. Experimental verification on FPGA

The performance of the design is compared with the existing work. Saravanan *et al.* [26], the reported delay is 7.205 ns and the frequency is 74.464 MHz on Xilinx Virtex-6 FPGA. Our design provides a maximum delay of 2.192 ns, and 215 MHz clock frequency, which means minimum delay and good frequency in comparison to existing work. Moreover, Diligent manufactured Zed board FPGA provides a number of expansion connectors that provide simple user access to the processing system and programmable logic I/Os.

5. CONCLUSIONS

The LFSR shift register shifts the signal from one bit to the subsequent most significant bit (MSB) and the outputs are connected in an exclusive OR fashion to form a feedback loop. The XOR operation is used to generate a linear feedback shift register by combining the outputs of two or more flip-flops and then feeding those outputs back to the flip-flop's inputs. The behavior is used in different communication system coding, error correction, and detection methods. In this work, we have simulated the same behavior for the Gold code sequence generator. The VHDL simulation of the LFSR modules is done successfully in the Xilinx ISE 14.7. The RTL and waveform simulation verify the functionality of the chip design. The behavior of the LFSR-1 and LFSR-2 is verified for the test input given in the simulation and test benches created for the testing of the designed chip functionality of the chip. The behavior model-based simulation is carried out for both LFSR and further applied for the gold sequence generator to provide 31bit output. The design is scalable and reprogrammable which can be extended based on the need of the communication system. The final design reports are verified in the simulation environment and the reported delay is 2.192 ns, and 215 MHz clock frequency. The reported frequency is significant for the high-speed communication system with the optimal delay reported. In the future, we are planning to implement large-scale input LFSRs with tap sequences that will produce a larger Gold code sequence generator. Future wireless communication provides everyone with a marginal throughput regardless of the complexity of the scenario or the density of the area. The LFSR produces sequences that are easily foreseeable due to their periodic character. The logic synthesis can be carried out on high-end FPGA so that it can support fast-switching communication systems with optimum hardware utilization in chip design.

ACKNOWLEDGEMENTS

The authors thank VLSI Design Lab, University of Petroleum and Energy Studies, Dehradun, India to carry out the simulation and synthesis work.




REFERENCES

- [1] S. Soliman *et al.*, "FPGA implementation of dynamically reconfigurable IoT security module using algorithm hopping," *Integration*, vol. 68, pp. 108–121, Sep. 2019, doi: 10.1016/j.vlsi.2019.06.004.
- [2] Z. Z. Aminuddin, I. H. B. Hamzah, A. A. A. Samat, M. Idris, A. F. A. Rahim, and Z. H. C. Soh, "An FPGA application of home security code using verilog," *International Journal of Reconfigurable and Embedded Systems (IJRES)*, vol. 11, no. 3, pp. 205–214, Nov. 2022, doi: 10.11591/ijres.v11.i3.pp205-214.
- [3] A. S. Babu and B. Anand, "Modified dynamic current mode logic based LFSR for low power applications," *Microprocessors and Microsystems*, vol. 72, Feb. 2020, doi: 10.1016/j.micpro.2019.102945.
- [4] R. Mishra, P. Kuchhal, and A. Kumar, "Effect of height of the substrate and width of the patch on the performance characteristics of microstrip antenna," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 5, no. 6, pp. 1441–1445, Dec. 2015, doi: 10.11591/ijece.v5i6.pp1441-1445.
- [5] K. H. Kaithan and S. J. Mohammed, "Implementing and designing a secure information system based on the DSSS gold sequence using matlab," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 10, no. 3, pp. 1455–1463, Jun. 2021, doi: 10.11591/eei.v10i3.2446.
- [6] Ompal, V. M. Mishra, and A. Kumar, "Zigbee internode communication and FPGA synthesis using mesh, star and cluster tree topological chip," *Wireless Personal Communications*, vol. 119, no. 2, pp. 1321–1339, Jul. 2021, doi: 10.1007/s11277-021-08282-w.
- [7] C. Bintjas *et al.*, "20 Gb/s all-optical XOR with UNI gate," *IEEE Photonics Technology Letters*, vol. 12, no. 7, pp. 834–836, Jul. 2000, doi: 10.1109/68.853516.
- [8] M. A. Esmail and H. Fathallah, "Physical layer monitoring techniques for TDM-passive optical networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 943–958, 2013, doi: 10.1109/SURV.2012.060912.00057.
- [9] A. S. Rawat, A. Rana, A. Kumar, and A. Bagwari, "Application of multilayer artificial neural network in the diagnosis system: a systematic review," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 7, no. 3, pp. 138–142, Aug. 2018, doi: 10.11591/ijai.v7.i3.pp138-142.
- [10] A. M. Gutierrez *et al.*, "Analytical model for calculating the nonlinear distortion in silicon-based electro-optic Mach-Zehnder modulators," *Journal of Lightwave Technology*, vol. 31, no. 23, pp. 3603–3613, Dec. 2013, doi: 10.1109/JLT.2013.2286838.
- [11] K. E. Stubkjaer, "Semiconductor optical amplifier-based all-optical gates for high-speed optical processing," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 6, no. 6, pp. 1428–1435, Nov. 2000, doi: 10.1109/2944.902198.
- [12] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Transactions on Information Theory*, vol. 13, no. 4, pp. 619–621, Oct. 1967, doi: 10.1109/TIT.1967.1054048.
- [13] J. E. García, G. Cotrina, A. Peinado, and A. Ortiz, "Security and efficiency of linear feedback shift registers in GF (2n) using n-bit grouped operations," *Mathematics*, vol. 10, no. 6, Mar. 2022, doi: 10.3390/math10060996.
- [14] M. Jayasanthi and R. Kalaivani, "Low-power DSSS transmitter and its VLSI implementation," *Annals of Telecommunications*, vol. 76, no. 7–8, pp. 537–543, Aug. 2021, doi: 10.1007/s12243-021-00837-z.
- [15] G. Giustolisi, R. Mita, G. Palumbo, and G. Scotti, "A novel clock gating approach for the design of low-power linear feedback shift registers," *IEEE Access*, vol. 10, pp. 99702–99708, 2022, doi: 10.1109/ACCESS.2022.3207151.
- [16] M. Saber and M. M. Eid, "Low power pseudo-random number generator based on lemniscate chaotic map," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 1, pp. 863–871, Feb. 2021, doi: 10.11591/ijece.v11i1.pp863-871.
- [17] H. Bae *et al.*, "High-speed counter with novel LFSR state extension," *IEEE Transactions on Computers*, vol. 72, no. 3, pp. 893–899, 2022, doi: 10.1109/TC.2022.3187343.




- [18] S. Hou, Y. Guo, and S. Li, "A lightweight LFSR-based strong physical unclonable function design on FPGA," *IEEE Access*, vol. 7, pp. 64778–64787, 2019, doi: 10.1109/ACCESS.2019.2917259.
- [19] S. Karunamurthi and V. K. Natarajan, "VLSI implementation of reversible logic gates cryptography with LFSR key," *Microprocessors and Microsystems*, vol. 69, pp. 68–78, Sep. 2019, doi: 10.1016/j.micpro.2019.05.015.
- [20] J. Lee and N. A. Touba, "LFSR-reseeding scheme achieving low-power dissipation during test," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 26, no. 2, pp. 396–401, Feb. 2007, doi: 10.1109/TCAD.2006.882509.
- [21] A. Kumar, A. Kumar, and A. Devrari, "Hardware chip performance analysis of different FFT architecture," *International Journal of Electronics*, vol. 108, no. 7, pp. 1124–1140, Jul. 2021, doi: 10.1080/00207217.2020.1819441.
- [22] G. Hu, J. Sha, and Z. Wang, "High-speed parallel LFSR architectures based on improved state-space transformations," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 3, pp. 1159–1163, Mar. 2017, doi: 10.1109/TVLSI.2016.2608921.
- [23] N. Gupta, A. Jain, K. S. Vaisla, A. Kumar, and R. Kumar, "Performance analysis of DSDV and OLSR wireless sensor network routing protocols using FPGA hardware and machine learning," *Multimedia Tools and Applications*, vol. 80, no. 14, pp. 22301–22319, Jun. 2021, doi: 10.1007/s11042-021-10820-4.
- [24] V. Raj, S. Janakiraman, S. Rajagopalan, and R. Amirtharajan, "Security analysis of reversible logic cryptography design with LFSR key on 32-bit microcontroller," *Microprocessors and Microsystems*, vol. 84, Jul. 2021, doi: 10.1016/j.micpro.2021.104265.
- [25] R. V. S. K. Dutt, R. Ganesh, and P. Premchand, "Neural net implementation of steam properties on FPGA," *International Journal of Reconfigurable and Embedded Systems (IJRES)*, vol. 10, no. 3, pp. 186–194, Nov. 2021, doi: 10.11591/ijres.v10.i3.pp186-194.
- [26] S. Saravanan, M. Lavanya, R. V. Sai, and R. Kumar, "Design and analysis of linear feedback shift register based on various tap connections," *Procedia Engineering*, vol. 38, pp. 640–646, 2012, doi: 10.1016/j.proeng.2012.06.079.

BIOGRAPHIES OF AUTHORS



Ms. Aakanksha Devrari    is B.Tech in Electronics and Communication Engineering from Uttaranchal institute of Technology, (UTU), Dehradun India 2011. M.Tech in VLSI Design, Faculty of Technology, Uttarakhand Technical University (UTU), Dehradun India in 2013. Pursuing Ph.D. (Electronics Engineering) in the domain of VLSI design. Her areas of interest are VLSI design, digital communication system. She has published more than 10 research papers in international journals and conferences. She can be contacted at email: adevrari@ddn.upes.ac.in.



Dr. Adesh Kumar    is working as Senior Associate Professor in the Department of Electrical and Electronics, Engineering "University of Petroleum and Energy Studies", Dehradun, India. He is B.Tech in Electronics and Communication Engineering from Uttar Pradesh Technical University Lucknow, India in 2006. M.Tech (Hons) in Embedded Systems Technology, from SRM University, Chennai in 2008. Ph.D. (Electronics Engineering) from University of Petroleum and Energy Studies (UPES), Dehradun India in 2014. He has also worked as Senior Engineer in TATA ELXSI LIMITED Bangalore and faculty member in ICFAI University, Dehradun. His areas of interest are VLSI design, embedded systems design, telecommunications and signal processing; He has published more than 100+ research papers in international peer reviewed journals (SCI/Scopus) and conferences. He is the reviewer of many SCI/SCIE and Scopus journals such as IEEE Transactions of Industrial Electronics, Wireless Personal Communications, Microsystem, Technologies, 3D research, Springer, Journal of Electronic Science and Technology, Journal of Visual Languages and Computing, Elsevier, World Journal of Engineering, and Emerald are few of them. He has supervised 7 Ph.D. scholars and 5 candidates are doing research under his supervision. He has chaired more than 10 sessions in international conferences and involved in the Ph.D. evaluation committee in UPES, India. Guest Editor: Special Issue "Intelligent Devices & Computing Applications" in Computer Systems Science and Engineering, Journal, Tech Science, 2022 (SCI Indexed). Guest Editor: Special Issue "Intelligent Communication and Smart Grid Automation Applications" in Intelligent Automation & Soft Computing, Journal, Tech Science, 2021 (SCI Indexed). Editor: Proceedings of Intelligent Communication, Control and Devices in Advances in Intelligent system and Computing (AISC), Book Series, Springer, Vol.989, 2020. (Scopus Indexed). He can be contacted at email: adeshmanav@gmail.com and adeshkumar@ddn.upes.ac.in.