Engineering, 2016, 8, 226-231
Published Online April 2016 in SciRes. http://www.scirp.org/journal/eng
http://dx.doi.org/10.4236/eng.2016.84019

Analysis, Design, and Test of CDMA LFSR with Offset Mask Using Standard ICs

Mouhamed Fadel Diagana[1], Serigne Bira Gueye[2]

[1]Engineering Institute of Computer Science and Telecommunications (I3T), Dakar, Senegal
[2]Department of Physics, Faculty of Sciences and Techniques, Cheikh Anta Diop University, Dakar, Senegal
Email: mouhamedfd@gmail.com, sbirag@gmail.com

Received 8 March 2016; accepted 24 April 2016; published 28 April 2016

Abstract

Hardware implementation of Linear Feedback Shift Register (LFSR) plays a great and very important role in communication systems, and in many security devices. In this paper, a design of LFSR with offset mask has been presented, for Direct Sequence Code Division Multiple Access (DS-CDMA) applications. Integrated electronic components have been used. An accessible model facilitating the synthesis on Printed Circuit Boards (PCB) and implementation on Field Programmable Gate Array (FPGA) is offered. In addition, a temporal and spectral analysis of the circuit is performed in order to validate the design. This latter facilitates the generation of pseudo-random codes based on LFSR and their integration into electronic systems.

Keywords

LFSR, CDMA, DS-CDMA, PCB, FPGA, Integrated Circuit (IC), Spread Spectrum (SS), Modular Shift Register (MSRG)

1. Introduction

LFSRs are used for DS-CDMA, errors detection and correction, and applications using pseudo-random sequences.

In this work, we first present the model that is used to design LFSR.

From this basic model we go further into the design using integrated electronic components.

Thus tests and checks have been performed on the circuit. Lastly the results have been analyzed and discussed.

For CDMA, LFSRs are mainly used for the multiple access scheme. The mask allows assignment of codes to identify users and base stations. LFSR is also helpful for generating quasi-random sequences and is used in hardware Built-In Self-Test (BIST) [1] [2], and security for Radio Frequency Identification (RFID) technologies

How to cite this paper: Diagana, M.F. and Gueye, S.B. (2016) Analysis, Design, and Test of CDMA LFSR with Offset Mask Using Standard ICs. *Engineering*, **8**, 226-231. http://dx.doi.org/10.4236/eng.2016.84019

[3]. However, their design is often done using only FPGA [4] [5]. Our goal in this work is not only to make a circuit board using standard integrated electronics components, but also to be able to move quickly on FPGA boards. In addition to this objective, a reliable method is given, allowing verification of the obtained signals.

2. Modeling of MSRG or Galois LFSR

Finite fields provide the necessary theory in designing LFSR [6] [7]. From a primitive polynomial, the equivalent circuit can be modeled with electronic components such as flip flops and XOR gates; each monomial indicates the feedback paths. For CDMA in the Q-channel the used polynomial is in a Galois configuration [8] as following:

$$P_Q^*(X) = 1 + X^3 + X^4 + X^5 + X^6 + X^{10} + X^{11} + X^{12} + X^{15} \tag{1}$$

The model describing this polynomial is shown schematically in **Figure 1**. The mask is also a circuitry with AND gates and XOR gates allowing achieve a particular shift [9] of the initial sequence. This model is the basis for concrete realization of the MSRG on integrated circuit.

The general form giving the output of each flip flop is defined by [8]:

$$Q_i(t+1) = \begin{cases} Q_{i-1}(t) \\ Q_{15}(t) \oplus Q_{i-1}(t), & \text{on feedback path} \end{cases} \tag{2}$$

where $Q_i(t)$ is the output of the *ith* register.

3. Design of the Q-Channel's LFSR

In this implementation, we move from modeling to realization. The following components have been used:

Two	**SN74273**:	*Octal D-Type Flip-Flop* (*With Clear*)
Six	**74HC86**:	*Quad* 2-*Input EXCLUSIVE-OR Gate*
Four	**74HC08**:	*Quad* 2-*Input AND Gate*

A benefit of this design is the availability of these components, and the reduction in the size of the device. The realized circuit is given in **Figure 2**.

This circuit can be divided into five main parts; the first is the LFSR. On the component U1SN74273, the outputs 3Q, 4Q, 5Q and 6Q are connected to U9SN74HC86. This is equivalent to blocks 3, 4, 5, 6 in **Figure 1**. Likewise on U2SN74273, the outputs 2Q, 3Q, 4Q are connected to U3SN74HC86, that's equivalent to blocks 10, 11, 12 in **Figure 1**. The second part represents the mask design; the third part allows selecting a determined mask with switch. The fourth part allows making unipolar to bipolar conversion [10] and the last permits spreading simulation with injected signal.

The selected mask corresponds to the sequence **100010010011000**; this sequence also corresponds to that chosen in the work [11]. Thus a comparison with simulation can be done.

On this circuit to avoid the lock-up state (the state where the register is blocked at 0) there are two solutions:

- A feedback logic that detects this state, and feeds one (up voltage) at the beginning (Q_1) [12]
- An OR gate and a signal to initialize the LFSR

For more flexibility in the practical realization, the second solution has been adopted. The register is initialized with a defined sequence.

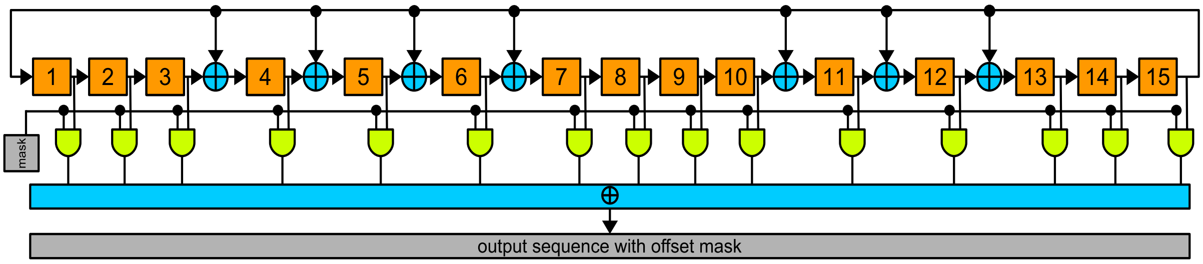

Figure 1. Q-Channel MSRG.

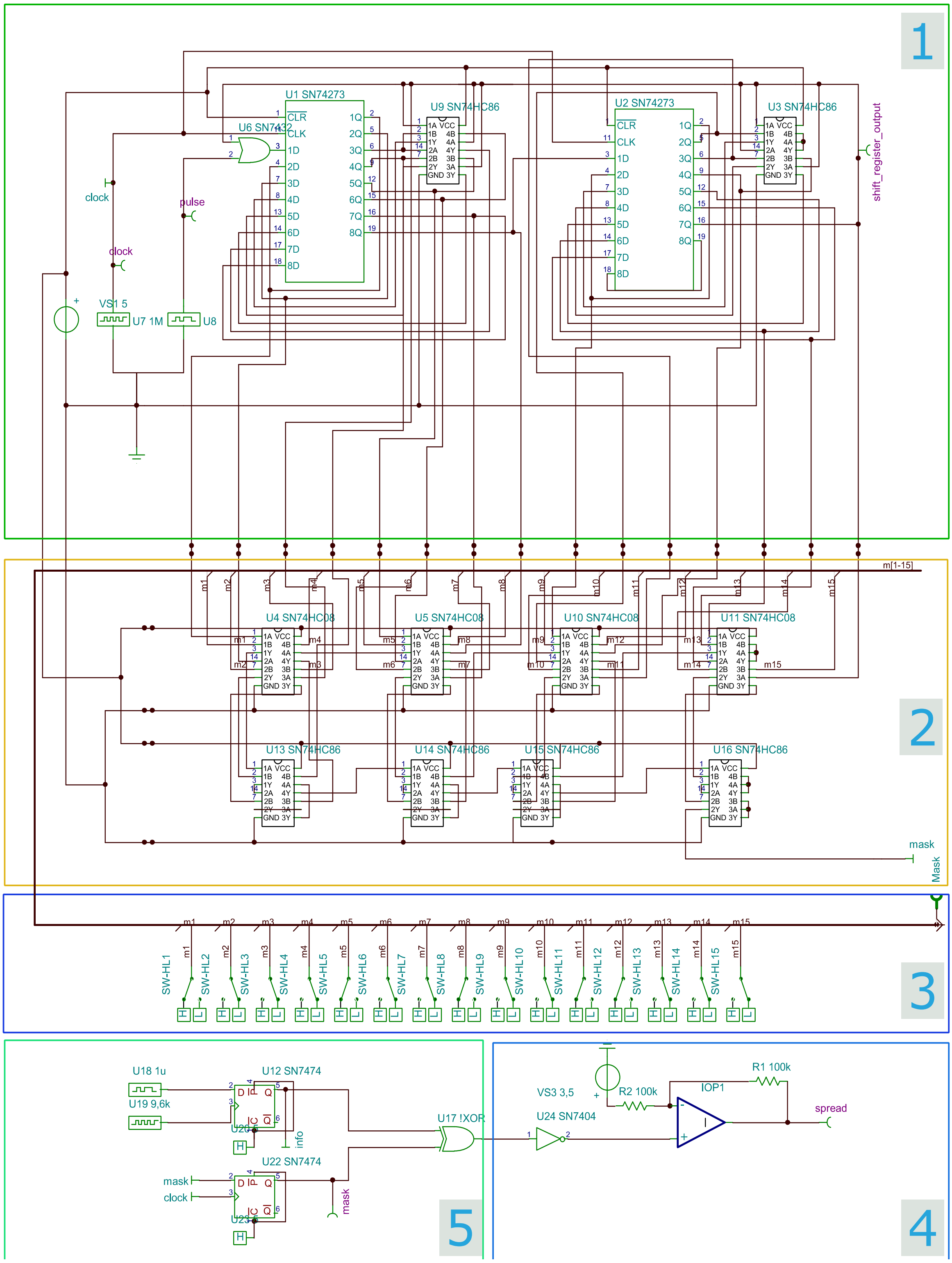

Figure 2. Design and simulation of Q-Channel MSRG with offset mask.

4. Tests and Results of the Circuit

Figure 3 describes the spreading process. It also shows the synthesis of the signals used on the timing diagram in **Figure 4**.

The signals srg_out, mask, and spread (in volt) are given respectively by blocks: LFSR, Mask and Spread.

To check the behavior of the circuit, and the conformity of the results with theory, long division of the polynomial is computed. We analyze timing diagrams at the output of the register and the mask **Figure 4** and **Figure 5**. The reciprocal polynomial corresponding to $P^*(X)$ is given by:

$$P_Q(X) = 1 + X^3 + X^4 + X^5 + X^9 + X^{10} + X^{11} + X^{12} + X^{15} \tag{3}$$

It helps build the LFSR in Fibonacci configuration. For this circuit we have fixed as the initial loading sequence **100000000000000** thus, the initial sequence of the LFSR output is given by the long division [8]

$$R(X) = \frac{X^{(15-1)}}{P_Q(X)} \tag{4}$$

X is an element of Galois Field {2}, and P a primitive polynomial. We get the following result:

$$R(X) = X^{14} + X^{17} + X^{18} + X^{19} + X^{20} + X^{22} + X^{24} + X^{25} + X^{26} + X^{28} + X^{30} + X^{31} + X^{33} + O(X^{34}) \tag{5}$$

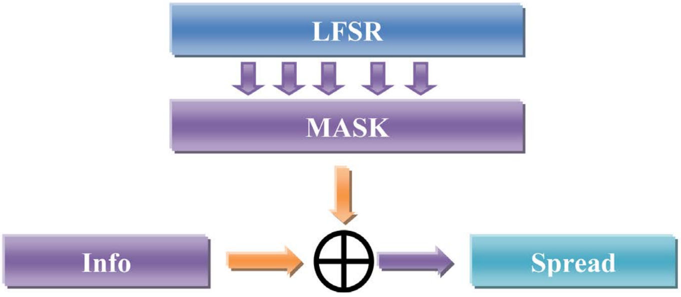

Figure 3. Spreading process in direct sequence CDMA.

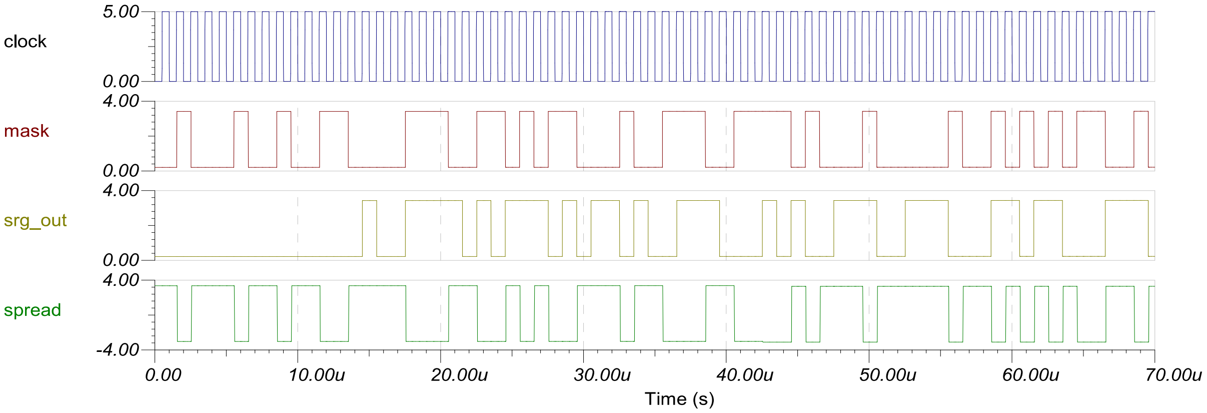

Figure 4. Timing diagram of the circuit.

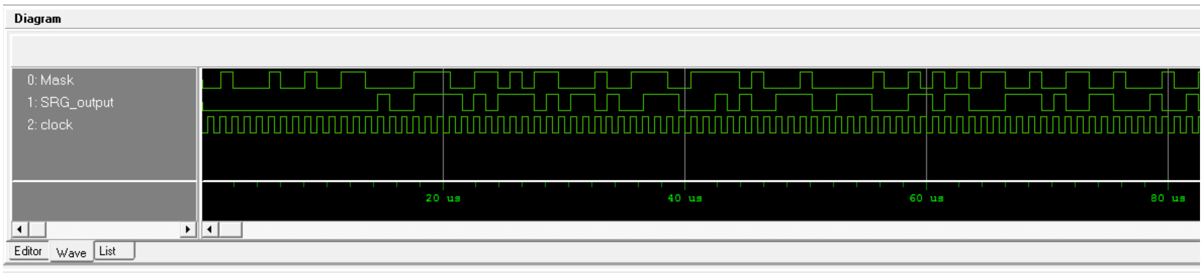

Figure 5. VHDL timing diagram of the circuit.

In this expression, each monomial indicates one element in the output sequence. $R(X)$ is equivalent to:

0000000000000010011110101110101101 and therefore confirms the obtained LFSR signals (srg_out, SRG_output) on timing diagrams **Figure 4** and **Figure 5**. By the same way, a verification of the mask signal can be performed.

Figure 5 shows the results under VHDL, it is also validated by simulation [11]. Further, it also shows the ability to make our design in FPGA boards.

We analyze the power spectrum **Figure 6** and the amplitude spectrum **Figure 7**, of an injected signal. The two graphs show the spreading of the signal spectrum in the 1 MHZ (clock) band and are also fully in accordance with the simulation.

Figure 6 shows a wanted feature both in spread spectrum systems and in scrambling devices [13], the output signal appear like a noise. However, the same processes of scrambling are used for descrambling and get the original information.

5. Conclusion

This herein presented design has several advantages. The use of simple integrated components to achieve these LFSR makes them more accessible and easy to embed on larger circuit architectures. In addition with the used tool [14], the VHDL code generation for this design is simplified, thereby allowing the use of FPGA boards. This design is efficient because of simplifying the realization of the corresponding PCB (Printed Circuit Board),

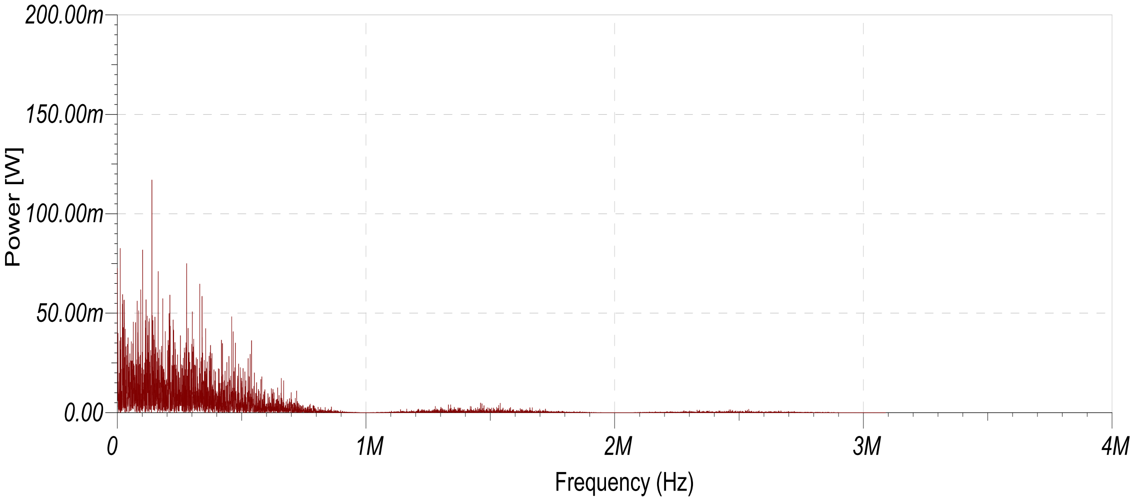

Figure 6. Power spectrum of spread signal.

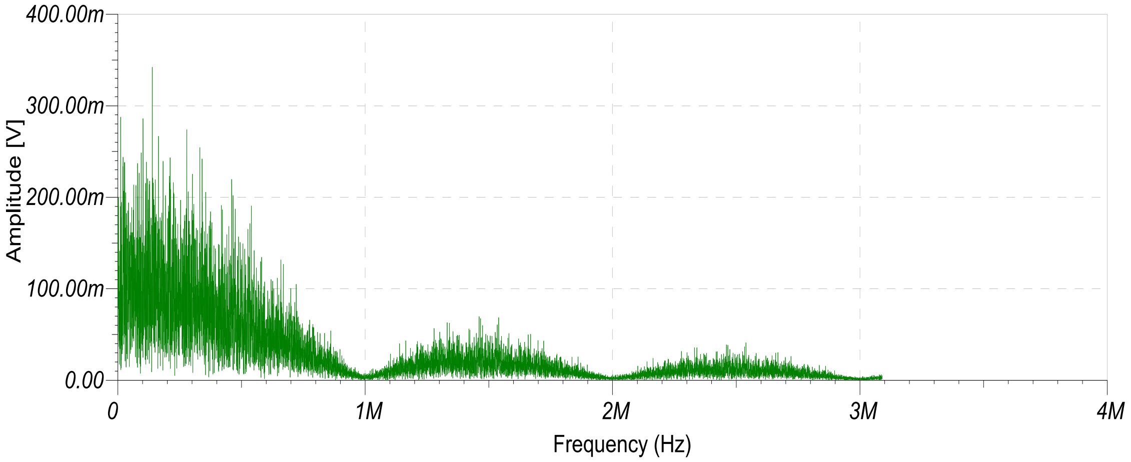

Figure 7. Amplitude spectrum of spread signal.

and its integration into information security devices.

References

[1] Ahmed, M.T. and Ali, L. (2012) Implementation of Fibonacci Test Pattern Generator for Cost Effective IC Testing. In 2012 *International Conference on Informatics*, *Electronics* & *Vision* (*ICIEV*), Dhaka, 18-19 May 2012, 1010-1015. http://dx.doi.org/10.1109/iciev.2012.6317462

[2] Islam, M.F., Ali, M.M. and Majlis, B.Y. (2013) FPGA Implementation of an LFSR based Pseudorandom Pattern Generator for MEMS Testing. *International Journal of Computer Applications*, **75**, 30-34.

[3] Melià-Seguí, J., Garcia-Alfaro, J. and Herrera-Joancomartí, J. (2011) Multiple-Polynomial LFSR Based Pseudorandom Number Generator for EPC Gen2 RFID Tags. *IECON* 2011—37*th Annual Conference on IEEE Industrial Electronics Society*, Melbourne 7-10 November 2011, 3820-3825. http://dx.doi.org/10.1109/iecon.2011.6119932

[4] Hwang, S.Y., Park, G.Y., Kim, D.H. and Jhang, K.S. (2010) Efficient Implementation of a Pseudorandom Sequence Generator for High-Speed Data Communications. *ETRI Journal*, **32**, 222-229. http://dx.doi.org/10.4218/etrij.10.1409.0047

[5] Bonde, V.V. and Kale, A.D. (2015) Design and Implementation of a Random Number Generator on FPGA. *International Journal of Science and Research*, **4**, 203-208.

[6] Simon, M.K., Omura, J.K., Scholtz, R.A. and Levitt, B.K. (1994) Spread Spectrum Communications Handbook (Volume 2). McGraw-Hill, New York.

[7] Mullen, G.L. and Panario, D. (2013) Handbook of Finite Fields. CRC Press, Boca Raton. http://dx.doi.org/10.1201/b15006

[8] Lee, J.S. and Miller, L.E. (1998) CDMA Systems Engineering Handbook. Artech House, Inc., Boston and London.

[9] Korowajczuk, L. and Xavier, B.S.A. (2005) Designing CDMA2000 Systems. John Wiley & Sons, Hoboken.

[10] Texas Instruments (2013) Bipolar +/−10V Analog Output from a Unipolar Voltage Output DAC. http://www.ti.com/lit/ug/slau525/slau525.pdf

[11] Diagana, M.F. and Gueye, S.B. (2015) Modeling and Simulation of CDMA Codes in Scilab. *International Journal of Communications*, *Network and System Sciences*, 8, 274-281. http://dx.doi.org/10.4236/ijcns.2015.87027

[12] Mohanty, S.P., Renuka Kumara, C. and Nayak, S. (2004) FPGA Based Implementation of an Invisible-Robust Image Watermarking Encoder. *Proceedings of* 7*th International Conference on Information Technology*, *CIT*, Hyderabad, 20-23 December 2004, 344-353. http://dx.doi.org/10.1007/978-3-540-30561-3_36

[13] Yoon, S.J., Suh, S.J. and Jung, M.C. (2013) U.S. Patent No. 8559480. U.S. Patent and Trademark Office, Washington DC.

[14] DesignSoft. TINA-The Complete Electronics Lab (Version 9). http://www.tina.com