A P-N SEQUENCE GENERATOR USING LFSR WITH DUAL EDGE TRIGGER TECHNIQUE

Mr. Nitin Kumar Naghwal[1], Abhishek Kumar[2]

[1] *M. Tech Student, School of Electronics Engineering, Lovely Professional University, Phagwara, Punjab*
[2]*Assistant Professor, School of Electronics Engieering, Lovely Professional University, Phagwara, Punjab*

Abstract. This paper represents the design and implementation of a low power 4-bit LFSR using Dual edge triggered flip flop. A linear feedback shift register (LFSR) is assembled by N number of flip flops connected in series and a combinational logic generally xor gate. An LFSR can generate random number sequence which acts as cipher in cryptography. A known text encrypted over long PN sequence, in order to improve security sequence made longer ie 128 bit; require long chain of flip flop leads to more power consumption. In this paper a novel circuit of random sequence generator using dual edge triggered flip flop has been proposed. Data has been generated on every edge of flip flop instead of single edge. A DETFF-LFSR can generate random number require with less number of clock cycle, it minimizes the number of flip flop result in power saving. In this paper we concentrates on the designing of power competent Test Pattern Generator (TPG) using four dual edge triggered flip-flops as the basic building block, overall there is reduction of power around 25% by using these techniques.

1 INTRODUCTION

Random numbers is essential to cryptography, cryptographic protocol AES, RSA, DES etc is depends on random number for encryption. Data security demands the generated number must be random and non deterministic known as pseudo random number. Pseudo number generator built from Linear Feedback Shift Register (LFSR) with judicious selection of the XOR taps feedback path. Pseudo random number generators generate a stream of numbers in a known pattern. The pattern is typically very long and it is hard to recognize the sequence of numbers is ordered. For example 128 bit LFSR requires to implement 32 PRNG with 96 bit are hidden protection comes from hidden number. Both hardware and software implementations of LFSRs are common. LFSR can be implemented in the hardware and it makes useful in applications that may require fast generation of a pseudo random sequence[12]

LFSR is preferred for test pattern generator and error correction due to its simple hardware structure. TPG is a device which generates uniqueness of patterns to test the Circuit under Test (CUT) shown in fig1. In computing, a linear-feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state. The most commonly used linear function of single bits is XOR. Thus, an LFSR is most often a shift register whose input bit is driven by the exclusive-or (XOR) of some bits of the overall shift register value. The initial value of the LFSR is called the seed, and because the operation of the

register is deterministic, the stream of values produced by the register is completely determined by its current (or previous) state. Likewise, because the register has a finite number of possible states, it must eventually enter a repeating cycle. However, an LFSR with a well-chosen feedback function can produce a sequence of bits which appears random and which has a very long cycle.
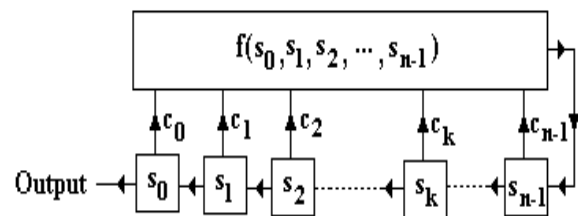

Figure 1. Random number generator

2 DETFF

In digital system clock signal has its special role; input clock signal controls the working rhythm of the chip. The clock signal controls flip-flops to sample and store their input data on active edge. To improve data rate clock frequency must increases, but in recent design performance of the flip-flop improved by increasing the active edge; in stead of accessing data on single edge accesson both edge. Dual edge triggered flip-flop (DETFF) can access data on both edges of the clock; it

---

[1]Corresponding author: nitinaghwal@gmail.com

enables the flip-flop to reduce the frequency half by maintaining same data rate. In VLSI working with high frequency result in high power consumption, DETFF draw attention to have high speed operation by lowering down the clock frequency. There is a reduction of 30-60% power saving compare to single edge triggered flip flop[8,9,10]. Fig2 (a) present a DETFF captures the input data at both positive and negative active edges of the input clock signal. Flip flop output is combined together using a multiplexer, at positive clock high latch output QH and at negative clock low latch output QL is routed to output port. As the timing of both the input signals i.e. clock and data matches, it provides the desired output, but whenever there are asynchronous signals or there is some mismatch in the timing than it leads to the errors due to setup and hold time violation. Fig2(b) the timing waveform of DETFF; QH latch on high and QL latches low, Q is combined effect of QH and QL. From waveform it seems that Q switches and each edge of clock and data transmission happens on both edges. It doubles the data rate known as double data rate flip flop.
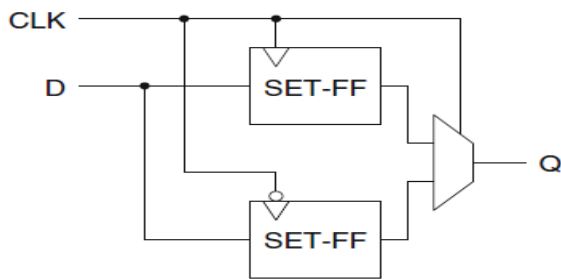

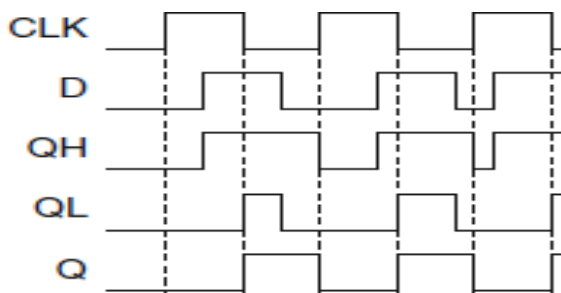**Figure 2(a).** Dual edge triggered flip flop[3]

Figure 2(b). Timing wave form of DDR flip flop[3]

3 LINEAR-FEEDBACK SHIFT REGISTER

LFSR is a linear feedback shift register whose input bit is a linear function of previous function that contains the signal through the register from one bit to the next most-significant when it is clocked. Figure 3 shows the block diagram of LFSR, a 4-bit LFSR generate 24-1 different non zero bit pattern by performing exclusive-OR gate on the outputs of two or more of the flip-flops and feeding those outputs back in to the input of one of the flip-flops.

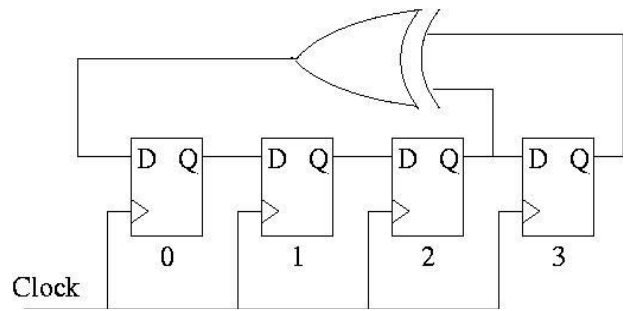An L bit LFSR generates the maximal length up to 2^L-1 combinations, figure4.
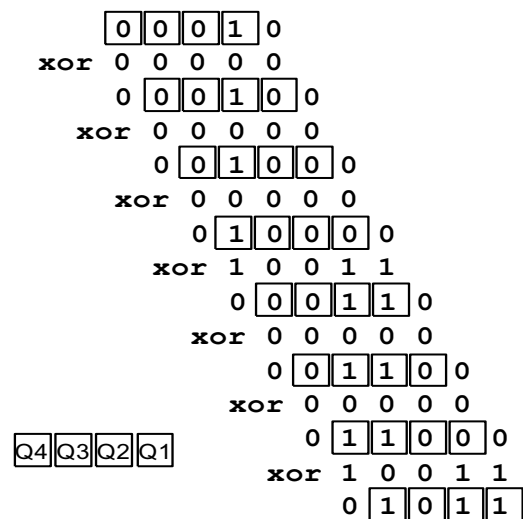

Figure 3. TPG using LFSR

Figure 4. Test pattern

4 LFSR WITH DET-FF

In this section a design of proposed FLSR has been discussed.

(i) High-level latch: A high level latch provides result on high level of clock. In fig5, on high level of clk Q=D. [9].
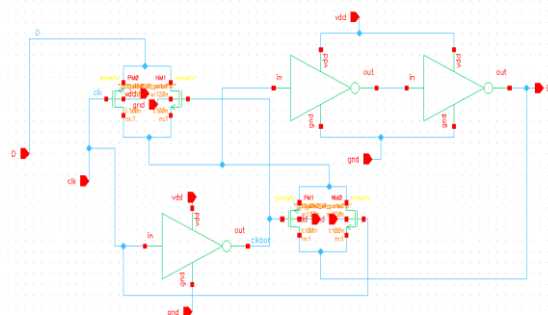

Figure 5. High-Level Latch

(ii) Low-Level Latch: A high level latch provides result on low level of clock. In fig6, on low level of clk Q=D.
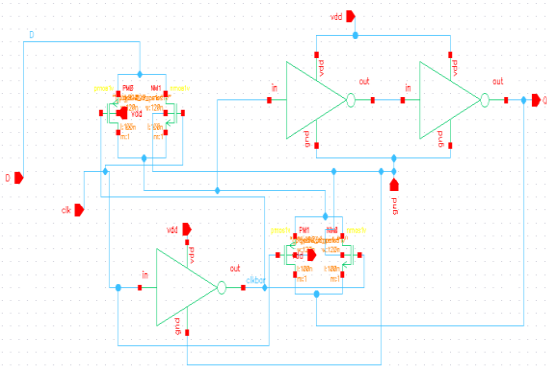
Figure 6. Low-Level Latch

(iii) Combiner Element: Here we have used the 2:1 MUX, which is used as the one of the combiner-element in the main circuit of DETFF. It combines the result of the high and low-level latch in the positive and negative clock.
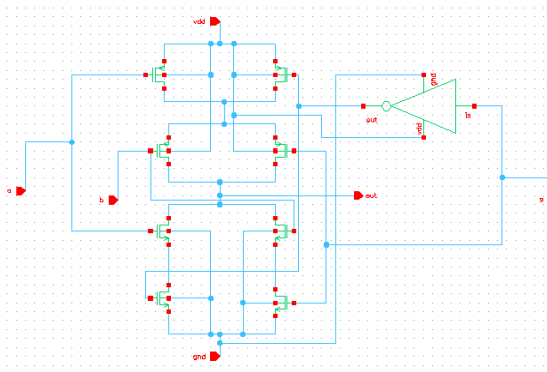

Figure 7. 2:1 MUX

(iv) Dual Edge triggered flip flop: A Dual edge triggered flip flop has two latch , one os high level sensetive and ither is low level. This DETFF require a combiner-element (mux) which combine the data accessed on high and low level of latch. Select line of multlplexer route the latch output to output trminal. MUX will select according to the clock provided as the select line. In detects the data on both of the levels and hence provides the same data at the output which is provided at the input of both latches Area of DETFF is about a half of that of edge-triggered FFs.[11] By combining all these blocks we perform the dual edge triggering and we got the same output which is provided at the input D.
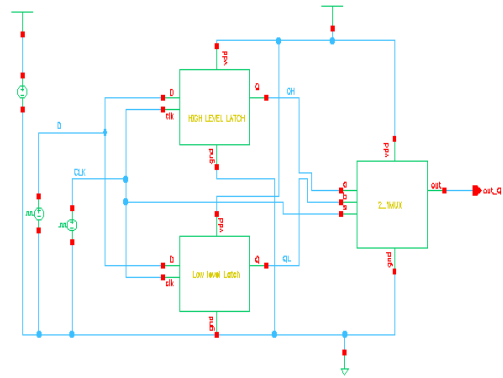

Figure 8. Basic DET FF

(v) Linear feedback shift register: fig 9 present a 4-bit LFSR using DDR flip flop. It consist of 4 flip flops so there will be total 16 patterns generated, but to initiate the LFSR we cannot feed the pattern of "0000" because the shift register would be stuck at this pattern because as we know that if we provide 0 at the input of the XOR gate than the output of XOR gate will be 0 always. So we have to provide any other pattern except all 0's. The LFSR is initiated by the input 0110, and it provides the output patterns as shown in figure 10 and 11. Figure 11 shows the output waveform of the LFSR. Cdence virtuoso circuit compser used for schematic design and Cadence spectre simulator using to obtained simulation result on cmos 90nm technology.

As the enable pin gets high the LFSR gets initialized. The first pattern is generated around 1.2 ns and about near to 3.2 ns all of the desired patterns has been generated, after this the pattern starts repeating. We analyzed that total time taken for the generation of the patterns is approximately 2ns.
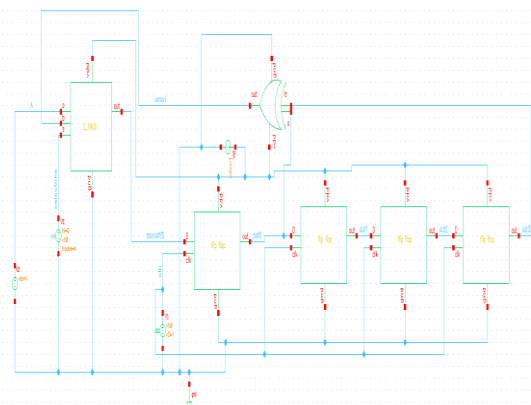

Figure 9. LFSR Schematic

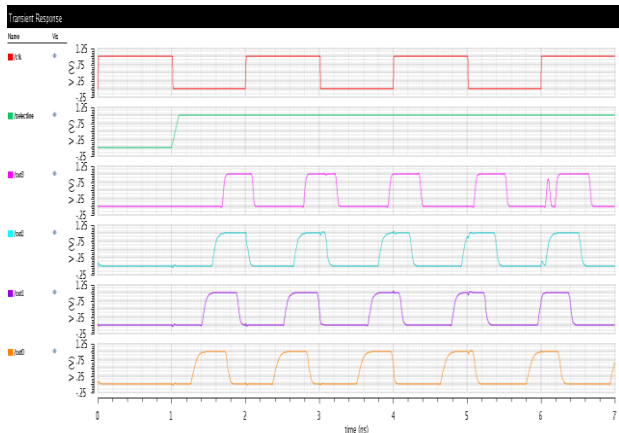| D_3	D_2	D_1	D_0
0	1	1	0
1	1	0	0
0	0	0	1
0	0	1	0
1	1	0	0
1	0	0	0
1	0	0	1
1	0	1	1
1	1	1	1
0	1	1	1

Figure 10. Output Patterns of LFSR

Figure 11. LFSR Output Waveform

5 SUMMARY AND CONCLUSIONS

In this paper a noble architecture of Dual edge triggered flip flop. Data capturing on both edge double the data rate. Double edge flip flop is an emerging technique for high speed data transmission. Designed LFSR generate random pattern on every clock edge, it significantly improves generation efficiency. Simulation result verifies that to obtained 10 random pattern a 4-bit LFSR consume 35.4uw and delay is 2ns.

REFERENCES

1. Kazuteru Namba, Takashi Katagiri, Hideo Ito,"Timing-Error-Detecting Dual-Edge-Triggered Flip-Flop" Journal of Electronic Testing, Vol. 29, pp 545-554, 2013.
2. Massoud Pedram, "A New Design for Double Edge-Triggered Flip-flops" International Journal of Electronics Communication and Computer Engineering Volume 4, pp 412-417, 2013.
3. Stojanovic, V.; Oklobdzija, V.G., "Comparative analysis of master-slave latches and flip-flops for high-performance and low-power systems," Solid-State Circuits, IEEE Journal of, vol. 34, pp.536-548, 1999.
4. Nedovic, Nikola; Aleksic, M.; Oklobdzija, V.G., "Conditional pre-charge techniques for powerefficient dual-edge clocking," Low Power Electronics and Design. Proceedings of the 2002 International Symposium, vol. 3, pp.56-59, 2002.
5. S. Wimer and I. Koren, "The Optimal fan-out of clock network for power minimization by adaptive gating," IEEE Trans. VLSI Syst., vol. 20, pp. 1772–1780, 2012.
6. Yasmeen Khan," Power Optimization of Linear Feedback Shift Register Using Clock Gating ," Volume 7, PP. 109-115, 2013.
7. S. Wimer and I. Koren, "The Optimal fan-out of clock network for power minimization by adaptive gating", IEEE Trans. VLSI Syst., vol. 20, pp. 1772–1780, 2012.
8. M. Muller, S. Simon, H. Gryska, A. Wortmann, and S. Buch, "Low power synthesizable register files for processor and IP cores", The VLSI J., vol. 39, pp. 131–155, 2006.
9. A. G. M. Strollo and D. De Caro, "Low power flip-flop with clock gating on master and slave latches", Electron. Lett., vol. 36, pp. 294–295, 2000.
10. J. Kathuria, M. Ayoub, M. Khan, and A. Noor, "A review of Clock Gating Techniques", MIT Int. J. Electron. and Commun. Engin., vol. 1, pp. 106–114, 2011.
11. Dr. Neelam R. Prakash, Akash, "Clock Gating for Dynamic Power Reduction in Synchronous Circuits", International Journal of Engineering Trends and Technology (IJETT), vol. 4,pp. 513-519, 2013.
12. P. Girard, L. Guiller, C. Landrault, and S. Pravossoudovitch, "A test vector inhibiting technique for low energy BIST design," in Proc. 17th IEEE VLSI Test Symp.,vol 3, pp. 407–412, 1999.
13. S. Manich, A. Gabarro, M. Lopez, J. Figueras, P. Girard, L. Guiller, C. Landrault, S. Pravossoudovitch, P. Teixeira, and M. Santos, "Low power BIST by filtering non-detecting vectors," J. Electron. Test.-Theory Appl., vol. 16, pp. 193–202, 2000.
14. F. Corno, M. Rebaudengo, M. Reorda, and M. Violante, "A new BIST architecture for low power circuits," in Proc. Eur. Test Workshop, vol 5, pp. 160–164, 1999.