ISSN:0975-9646

Design and Implementation of Pseudo Random Number Generator in FPGA & CMOS VLSI

Chandra Sekhar.K[1], Unitha.Pailu[2], Aradada.Sirisha[3]
Assistant.Professor[1,2,3]
Dept. of Electronics & Communication Engineering,
Raghu Institute of Technology,
Visakhapatnam, INDIA.

***Abstract*— Pseudo Random number Generator(PRNG) is used in various cryptographic applications such as Bank Security, Generation of Keys which are used for Encrypting or Decrypting Messages, Networking etc. The Random number generator discussed in this paper uses the concept of Shift registers and is designed using Maximum length feedback polynomial, which is more advantageous when compared to other Random number generators or Counters that are used in Cryptography. In this paper the design and implementation of PRNG using Field programmable gate array (FPGA) is explained and it is compared with other counters to observe its performance in various aspects . PRNG is also implemented using different topologies in CMOS to reduce the Power Consumption .**

***Keywords*— PRNG, FPGA, Maximum Length Feedback Polynomial**

I. INTRODUCTION

In Shift Register input bit is driven by the exclusive-or (XOR) of some bits of the overall shift register value. The initial value given to the Shift Register is called the seed[1]. The feedback function should be selected in such a way so that it produces a sequence of bits which has a very long cycle and random in nature. The repeating sequence of a Shift Register allows it to be used as a Counter, or as a Random number generator however it is necessary to ensure that the Shift Register never enters an all-zeros state. PRNG designed using Shift Registers have simpler Feedback logic than natural Gray counters or Binary code counters, and operates at higher clock rates[2]. Binary counters are designed using Flip-Flops , half adders, and a high-speed carry chain. The delay associated with such counters depends on the number of bits in the adder/carry chain circuit. In contrast, PRNG designed using Shift Register use only XOR gates and Flip-Flops. The delay associated is independent of the number of bits in the counter. Binary, Gray Counters suffer from the problems of glitches, speed, Power Consumption and delay. They produce not only glitches, which increase power consumption but also increases the complexity of design.

II. MAXIMUM LENGTH FEEDBACK POLYNOMIAL

Maximum-length Feedback Shift Register produces an maximum sequence i.e. it cycles through all the possible 2^n-1 states within the Shift Register[4]. The only signal necessary to generate the Random patterns is the Clock. Shift Register outputs are traditionally labelled from 1 through n, with 1 being the first stage of the shift register, and n being the last stage[4]. This is different from the conventional 0 to (n-1) notation for binary counters.

A. Rules for Selecting Maximum Length Feedback Polynomial

Shift Registers produce the Maximum Length sequence, when the characteristic polynomial used in the design is of Maximum Length[3]. The choice of Shift register length, gate type, Maximum length logic, and tap positions allows the user to control the implementation and feedback of the Shift Register, which, in turn, controls the sequence.

The following things have to be noted while selecting the Maximum Length Feedback Polynomial

- The initial value of the Shift Register is called the seed. The seed value can be anything except all 0s i.e., the Pseudo Random sequence must start in a non-zero sequence.
- The 'One' in the Maximum length Feedback sequence corresponds to the principal input of the shift register.
- The Shift Register will only be Maximum length if the numbers of taps are even. Tap values should be relatively prime. The first and last taps should always be connected as input and output taps respectively.
- Mirror Sequence exists for the given tap sequence and can be more than one tap sequence for a particular .

III. IMPLEMENTATION OF SHIFT REGISTER BASED PRNG IN FPGA AND CMOS VLSI

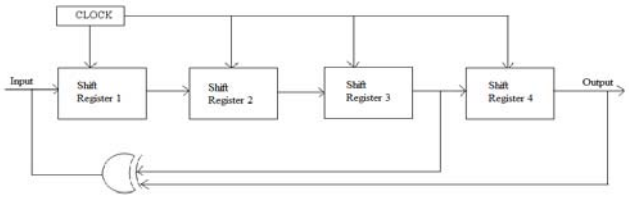

Figure 1: 4 Bit Pseudo Random Number Generator

The above Figure is the basis for the design of PRNG in both FPGA and in CMOS VLSI. The design is carried out in two phases. In the first phase the Circuit is designed and implemented in FPGA. The target device used in the design is Xilinx Spartan XC3S 500e . Simulation and

Synthesis is performed using Xilinx and the results are compared with other counters. Various parameters like Speed, number of Flip-Flops required , LUTS required , Delay etc are compared in this phase and Verilog HDL is preferred for programming because it is less complex and widely used. In the second phase the paper mainly focuses on the transistor level design of the PRNG. This is performed using Mentor Graphics HEP-1 tool.

A. DESIGN ASPECTS OF PRNG

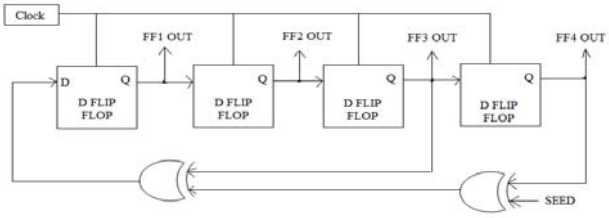

Figure 2: 4 Bit Pseudo Random Number Generator (Flip Flop Model)

The PRNG designed in the Figure 1 is a combination of Shift Registers and XOR Gates. Shift Registers are nothing but Flip Flops. By changing the Flip Flop Designs, the power consumption of the PRNG can also be reduced to a considerable extent finally producing a low power consuming VLSI Chip[3]. There are many Topologies for the design of Flip-Flops. Some of the prominent Flip-Flop Topologies have been discussed in this paper.

B. Design of D-Flip Flop using NAND Logic

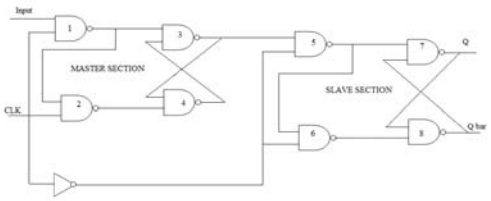

Figure 3: Design of D Flip Flop using NAND Logic

The working of the above circuit can be explained in the following fashion the first 4 NAND gates form the Master section and the last 4 NAND gates form the Slave Section, the Master and Slave section are controlled by the inverter gate. When clock is active high the Master section works and the output is produced and when the clock is active low the Slave Section works and the output is retained by the counter[5]. Thus the counter functions in both the clock cycles.

C. DESIGN OF D FLIP FLOP USING TRANSMISSION GATE

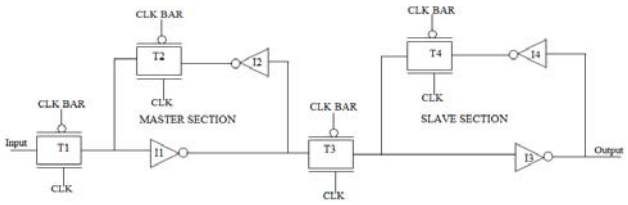

Figure 4: Design of D Flip- Flop using Transmission gate logic

The flip-flop is realized by using two transmission gate based latches which operate on complementary clock. Although this structure has high-speed and consumes low power, it is sensitive to overlap of the clocks[5]. At the negative edge transition of the clock, transistors T1 and T4 are in ON state and transistors T2 and T3 are in OFF State. At this time the slave maintains a loop through the two inverters I3, I4 . Thus the previous triggered value from Din is stored in slave. At the same time master latches next state but as T3 is in OFF state it is not passed to slave. At the positive clock edge T2 and T3 are turned ON and new latched value passes to slave through the loop of two inverters I1, I2 and T2 gate.

D. DESIGN OF D FLIP FLOP USING PASS TRANSISTOR

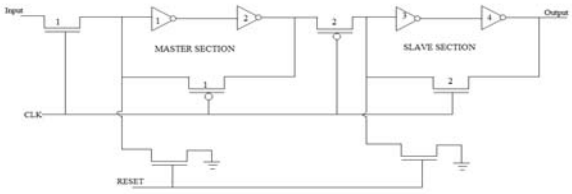

Figure 5: Design of D Flip Flop using Pass Transistors

The most compact implementation of edge triggered Flip Flop is based on pass transistors and inverters as shown in Figure 4.The two chained inverters are in memory state when the PMOS loop transistor is turned on, that is when clock is equal to zero. Other two chain inverters on the right hand acts exactly in opposite way, and the reset function is obtained by direct ground connection of the Master and Slave memories, using NMOS devices[5]. When the Reset signal is activated irrespective of the input applied the output of the Flip- Flop will be zero.

E. DESIGN OF D FLIP FLOP USING 8T MODEL

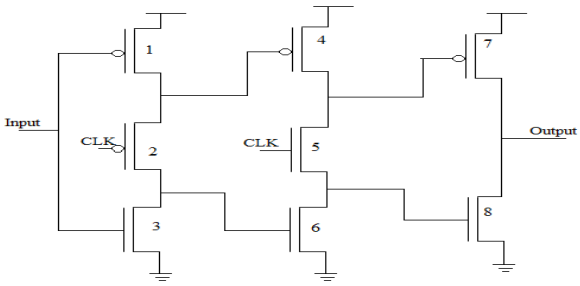

Figure 6: Design of D Flip Flop using 8T model

To overcome the problem of Clock Skews and distributing Clock signals , a development of NORA-CMOS technique is introduced using True Single Phase Clock (TSPC) CMOS circuit technique. True Single Phase Clock flip-flops have the advantage of single clock distribution, High Speed , small area for clock lines and no clock skew. The Figure shows the implementation of 8-transistor positive edge-triggered D flip-flop using split-output TSPC latches.

IV. SCHEMATIC DIAGRAMS

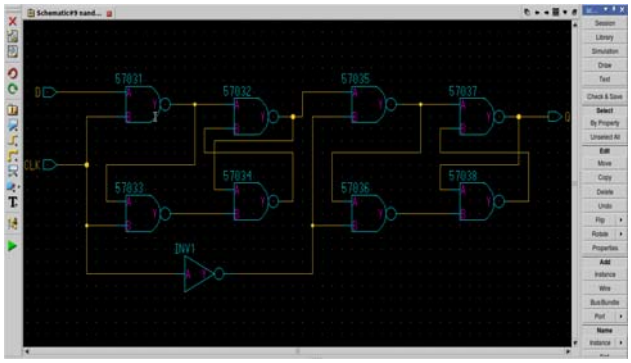

Figure 7: Schematic of D Flip Flop using Nand gates

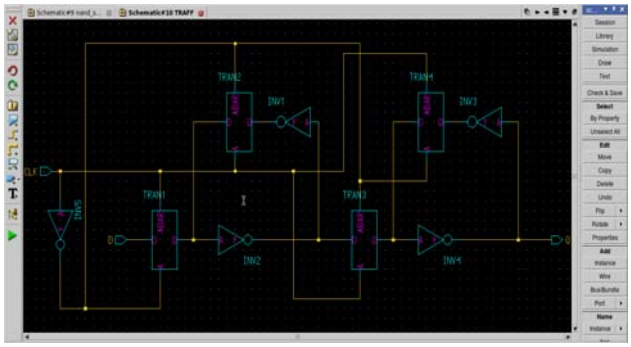

Figure 8 : Schematic of D Flip Flop using Transmission gates

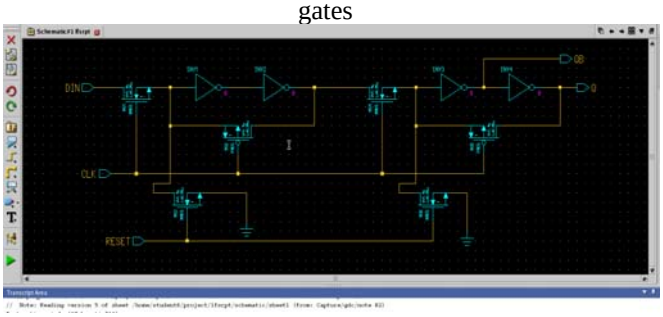

Figure 9: Schematic of D Flip Flop using Pass Transistor gates

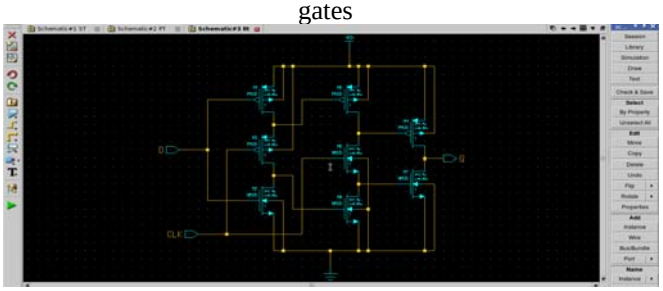

Figure 10 : Schematic of D Flip Flop using 8T Model

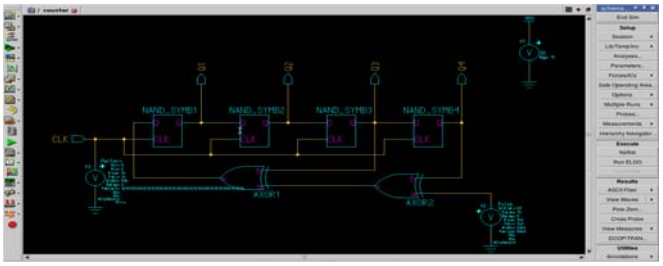

Figure 11 : Schematic of LFSR Counter designed using Mentor Graphics tool

V . RESULTS AND COMPARISON

Table 1: Results for Selected Device XC3S500E

	4 Bit Counters			8 Bit Counters		
Parameter	**Binary**	**Gray**	**LFSR**	**Binary**	**Gray**	**LFSR**
No of Slices	2	3	2	4	8	4
No of Flip Flops	4	4	4	8	8	8
No of 4 i/p LUT'S	4	6	1	8	15	1
Total Pins	6	7	6	10	11	10
Delay	6.621 ns	7.726ns	6.534ns	6.607 ns	7.799 ns	6.534 ns
	16 Bit Counters			**32 Bit Counters**		
Parameter	**Binary**	**Gray**	**LFSR**	**Binary**	**Gray**	**LFSR**
No of Slices	8	17	9	17	34	9
No of Flip Flops	16	16	16	32	32	32
No of 4 i/p LUT'S	16	31	1	33	63	1
Total Pins	18	19	18	34	35	18
Delay	6.843 ns	8.035 ns	6.534 ns	9.929 ns	10.268 ns	6.534 ns

Table 2 : Comparison of 4 Bit LFSR Counter Power Consumption for different Topologies

Sno.	Topologies	Transistors per Flip-Flop	Power Consumed
01	Nand	34	4.8537 nWatts
02	Transmission gate	18	3.3153 nWatts
03	Pass Transistor	14	2.6367 nWatts
04	8T	8	0.3360 nWatts

A. Simulation Results

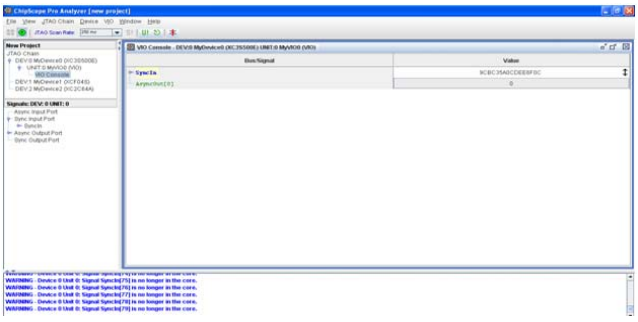

Figure 12: Simulation Result for 64 Bit PRNG in FPGA

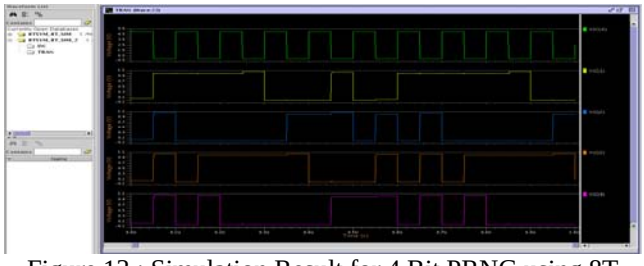

Figure 13 : Simulation Result for 4 Bit PRNG using 8T Model

VI. CONCLUSION

Shift Register based Pseudo Random Number Generator has many advantages over other counters in terms of Speed , Area and Hardware. It is preferable when good logic density is to be maintained during fabrication process, while obtaining power optimization and reducing the propagation delay & glitches of the circuit . The Comparison results of different Counters with Shift Register based PRNG is provided in this paper and it is implemented using different Flip-Flop Topologies. The power consumption for different topologies is verified using Mentor Graphics tool. The power consumption can further be reduced by using other available topologies there by making it more efficient for the chip design.

REFERENCES

[1]. Rajendra S.Katti, Xiaoyu Ruan and Hareesh Khattri, "Multiple output Low Power Linear Feedback Shift Register Design," IEEE Transactions on Circuits and Systems-I, vol. 53, No.7 July 2006.

[2]. Shiv Dutta Mishra, Prof. Anurag Shrivastav "Design and Analysis of FPGA based cryptographic N-bit parallel LFSR", *International Journal of Latest Trends in Engineering & Technology (IJLTET), NOV 2013*, Vol. 3, Issue 2, ISSN. 2278-621X.

[3] . Goresky, M. and Klapper, A.M. Fibonacci and Galois representations of feedback-with-carry shift registers, *IEEE Transactions on Information Theory*, Nov 2002, Volume**:** 48, On page(s): 2826 – 2836.

[4] Panda Amit K, Rajput P, Shukla B, "Design of Multi Bit LFSR PNRG and Performance comparison on FPGA using VHDL", *International Journal of Advances in Engineering & Technology (IJAET), Mar 2012*, Vol. 3, Issue 1, pp. 566-571.

[5]. Doshi N. A., Dhobale S. B., and Kakade S. R., "LFSR Counter Implementation in CMOS VLSI", World academy of Science and Technology, 48 2008.