E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

# ADVANCE PARALLEL LFSR FOR CRYPTOGRAPHY

Shiv Dutta Mishra[1], Prof. Anurag Shrivastav[2]
[1] *Research Scholar ME (VLSI Design), Shri Shankaracharya Group of Institutions, chattisgarh, India*
[2] *Faculty of Engineering & Technology, Electronics and Instrumentation, Shri Shankaracharya Group of Institutions, chattisgarh, India*
[1] *sdmishra1982@gmail.com*

**ABSTARCT:**
**The FPGA based implementation of advance parallel LFSR Pseudo Random Sequence Generator formed combining a parallel LFSR and counter using XOR gate is presented in this paper that can be used in cryptography for securing the Internet traffic in places where low memory utilization and high level of security is required. Random numbers form the centerpiece of cryptography provided the seed that the random number generator provides remains secretive and a high degree of randomness is maintained. For high degree of randomness multiple LFSR are often combined. FPGA is especially popular for prototyping integrated circuit designs and to develop and simulate a sophisticated digital circuit, realize it on a prototyping device, and verify the operation of its physical implementation. As these Technologies have become accepted mainstream practice so that it is possible to use a PC and an FPGA prototyping board to construct a digital circuit. The design of advance parallel LFSR circuit was implemented in a Vertex 5 series (xc5vlx30-3-ff324) target device with the use of Verilog as the hardware description language.**

***Keywords:*** *LFSR, FPGA, HDL, Cryptography and Verilog.*

## 1. INTRODUCTION

N-bit maximum length linear feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state is shown in fig (1). The only linear function of single bits is XOR, thus it is a shift register whose input bit is driven by the exclusive-or 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. The arrangement of taps for feedback in an LFSR can be expressed in finite field arithmetic as a polynomial mod 2. This means that the coefficients of the polynomial must be 1's or 0's. This is called the feedback polynomial or characteristic polynomial. For example, in 4 bit LFSR if the taps are at the 4th and 3rd bits, then the feedback polynomial is x4 +x3 +1.Flip-flops are clocked in every clock cycle and only one bit of information is generated per clock cycle. The output can be taken from input or output of any flip-flop.

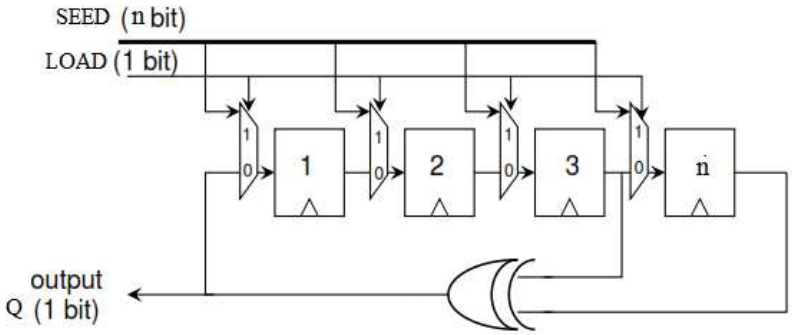


Figure 1 Linear feedback shift register (LFSR)

The construction of pseudo-random number generator (PRNG) is based on linear feedback shift register (LFSR). This class of generators can be very effectively implemented in hardware, is capable to generate very long pseudorandom sequences with a high-quality statistical distribution.

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

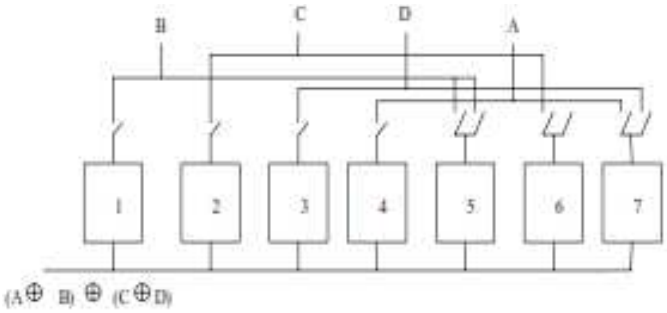


Figure 2 Single output realization of F(X) = 1+ X4 + X7.

The parallel architecture of an LFSR designed by M. Lowy [1] is shown in fig (2).Individual cell in the register do not change value except when updated once every N clock cycle instead i.e. only one flip-flop is updated every clock cycle and instead of the bits moving from left to right, the tap of XOR tree move from right to left in the direction of preceding cell. It reduces dynamic power consumption and can generate more than one bit output per clock cycle. The M. Lowy architecture uses an

1. N-phase generator that generates N signal to clock flip flop and is realized by johnson counter of length N/2.
2. Control unit that control the operation of M+N switches and is realized by M+N OR gate.

M. E. Hamid and C. I. H. Chen[2] proposed a new form of polynomial with two coefficients having the following format:

$$F(X) = 1 + X^{N/2} + X^{N}$$

Where, N is the order of the polynomial shown in fig (3). The proposed polynomial reduces the number of switches required as well as a 3% increase in number of distinct patterns generated.

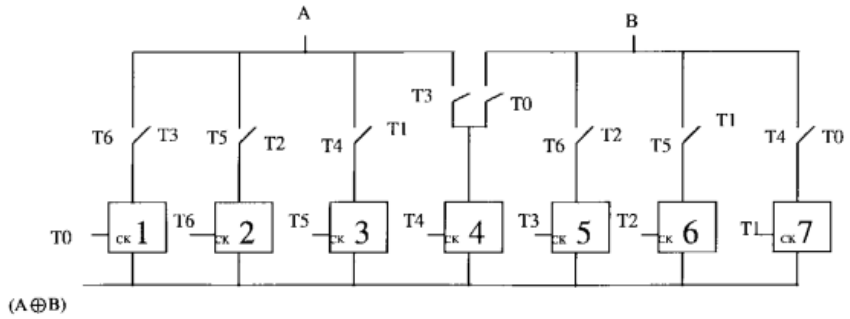


Figure 3 Single output realization of F(X) = 1+ X4 + X7.

Abdullah Mamun and Rajendra Katti [3] proposed design is shown in fig (4) in which additional XOR gates are used and they are permanently connected to the respective flip-flops where as in both Lowy's design and Hamid's design, taps move. It is very simple in design, reduces power consumption significantly, and eliminates the control unit.

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

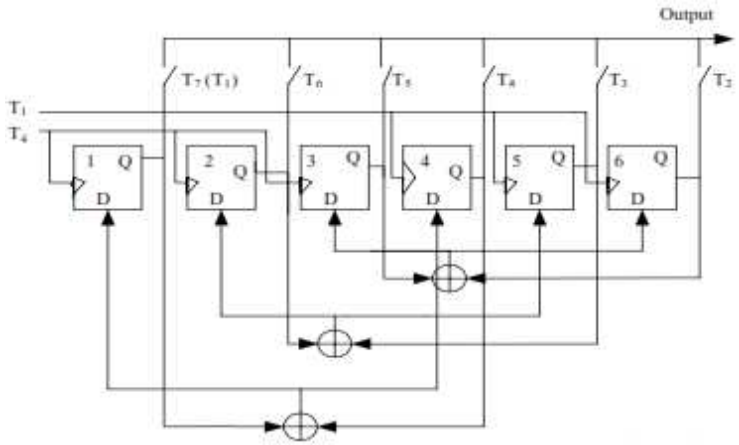


Figure 4 Single output realization of F(X) = 1+ X3 + X6.

Let us use the polynomial F(X) = 1+ X3 + X6. Table 1 shows the storing method of calculated results in order to obtain the parallel implementation. In cycle 1, XOR result of flip-flops 3 and 6 (which is calculated in the previous cycle) is stored in flip-flop 6. Similarly in clock cycle 2, 3, 4, 5, and 6 XOR results of flip- flops (2,5); (1,4); (6,3); (5,2); and (4,1) should be stored in flip- flop 5, 4, 3, 2, and 1 respectively. It should be noted that XOR results of flip-flop (3,6) are same as XOR results of (6,3). Thus number of XOR gates needed is 6/2 = 3.

Table 1 Update of flip-flops, F(X) = 1+ X3 + X6

| **Clock cycle** | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| **XOR result of** | 6,3 | 5,2 | 4,1 | 6,3 | 5,2 | 4,1 |
| **Updated FF** | 6 | 5 | 4 | 3 | 2 | 1 |

Consider polynomial 1+ x2 + x5 for architecture proposed by M. Lowy for obtaining multiple output in a single clock cycle using M. E. Hamid and C. I. H. Chen[2] polynomial. The control signal Ti (i = 1, 2 ... N), which is used to connect the shift register to the output tap, is a sequentially occurring waveform. The control signal is high for only i mod N clock cycle, where N is the length of the LFSR. The operations (5,2) and (4, 1) are performed at T1, where (x, y) denotes XOR operation of x and y. The value of the XOR operation is the output of the LFSR, obtained at A and B respectively. The outputs A and B are feedback and stored in flip-flop 5 and flip-flop 4 respectively at T2 cycle. At T2, operations (3, 5) and (2, 4) are performed. These values are stored in flip-flop 3 and flip-flop 2 respectively. The overall operations can be summarized as shown in Table2.

Table 2.Update of flip-flops, F(X) = 1+ X2 + X5

| **Clock Cycle** | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **XOR Result of Output A** | 5,2 | 5,3 | 3,1 | 4,1 | 4,2 |
| **XOR Result of Output B** | 4,1 | 4,2 | 5,2 | 5,3 | 3,1 |
| **Updated FF** | A—2 B—1 | A—5 B—4 | A—3 B—2 | A—1 B—5 | A—4 B—3 |

With the multiple output architecture, a polynomial, of the form 1 + xk1 + xk2 + xk3 + ..... + x N can generate. k outputs in a single clock cycle. In the case of 1+ x2 + x5, 2 outputs can be obtained in a single clock cycle. In order to produce all the outputs, 5 clock cycles are required [4]. The same polynomial, 1+x2+x5, implemented in the architecture as proposed by Katti are as shown in Fig. (3). At T1, operations (5, 2) and (4, 1) are performed. Values of these operations are stored in flip- flop 5 and flip-flop 4 respectively at T2. At T2, operations (5, 3) and (4, 2) are performed. The result of the XOR operation is stored in flip-flop 3 and flip-flop 2

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

respectively at T3. At T3, only one operation (3, 1) is performed, and the result is stored in flip-flop 1 at T1. The operation can be summarized as shown in Table 3.

Table 3 Update of flip-flops, F(X) = 1+ X2 + X5

| **Clock Cycle** | 1 | 2 | 3 |
|---|---|---|---|
| **XOR Result Of Output A** | 5,2 | 5,3 | 3,1 |
| **XOR Result Of Output B** | 4,1 | 4,2 | |
| **Updated FF** | A—5<br>B—4 | A—3<br>B—2 | A—1<br>B—5 |

In this architecture, the numbers of control signals required are N / k1, where N is the length of LFSR and k1 is the number of simultaneous outputs. In this example, 3 control signals are needed, and all the outputs are produced in 3 clock cycle [4].Advantages of Abdullah Mamun and Rajendra Katti [3] design.

1. Only N/2 XOR gates are required.
2. No need to have N-phase generator. T2 can be generated by inverting the clock.
3. No need to have multi-clock flip-flops, which is required by earlier methods.
4. No switches are required, whereas for only double output generation Lowy's method requires about 3*(N+M) switches.
5. No extra XOR gates are required for multiple outputs, whereas previous methods require doubling the XOR gate requirement for double output generation.
6. As the clock rate is reduced by N/2, supply voltage can be reduced which in turn reduces power consumption.

In the proposed design a parallel LFSR is formed by using single XOR gate and is permanently connected to the respective flip-flops with bits moving LSB to MSB flip flop and position of taps are given using M. E. Hamid and C. I. H. Chen polynomial produces N bit parallel output in a single clock. For the odd-order polynomial, the LFSR can be used for either ceiling or floor value of N/2. Outputs from the LFSR and the Counter are combined by an XOR gate. It can be used in cryptography where low memory utilization and high level of security is required [5]. To increase the number of state advance parallel LFSR is used formed by combination of parallel PRNG.

This paper examines the full procedure of Advance parallel LFSR using a high-level hardware description language; Verilog, combined with the usage of FPGA technology. In section 2 we have proposed design of Advance parallel LFSR and in Section 3 the complete design was synthesized for FPGA devices Virtex 5. The design is implemented and verified on a Virtex 5 FPGA development board from Xilinx using device (xc5vlx30-3-ff324) and then simulated using model Sim ISE simulator. In section 4 conclusions are given.

## 2. PROPOSED ADVANCE N BIT PARALLEL LFSR

The Block diagram of proposed advance N bit parallel LFSR is shown in fig 5. The proposed advance parallel LFSR using N bit parallel linear feedback shift register (LFSR) and N bit parallel Counter clocked by a single clock and selected outputs from the LFSR and the Counter are combined by an XOR generating the final random signal. The proposed advance parallel LFSR is mainly divided into two parts

- N bit parallel LFSR
- N bit parallel Counter

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

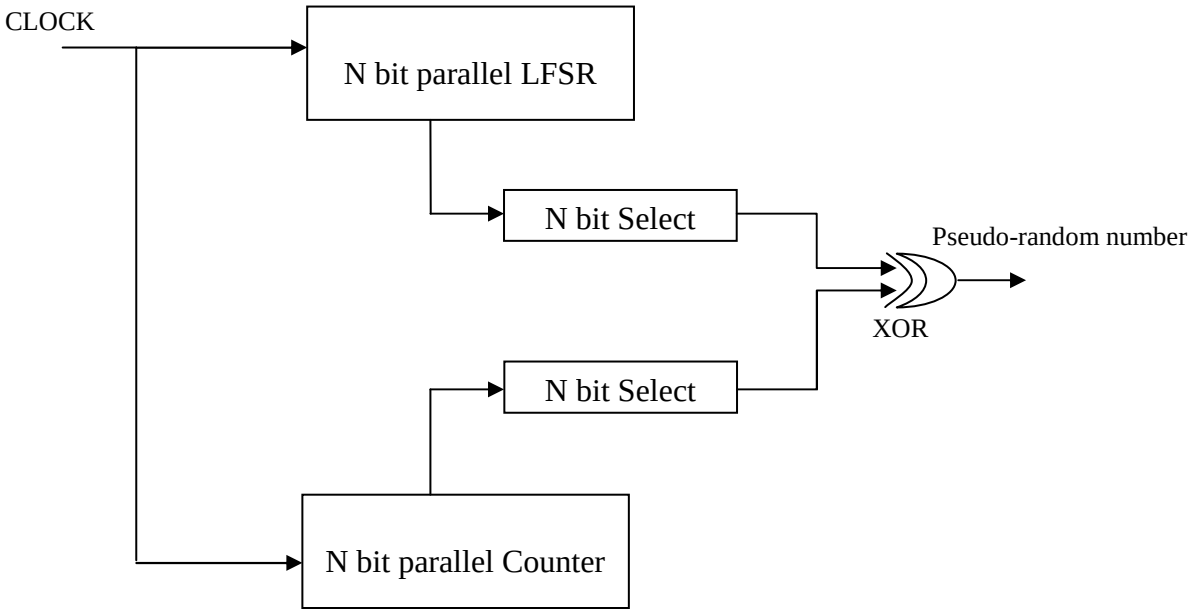


Figure 5 Block diagram of proposed advance N bit parallel LFSR

### *2.1. N bit parallel LFSR*

The designing of proposed N bit parallel LFSR is done by the help of N flip flop, the flip flop used is D flip flop and a XOR gate [6]. Output is taken from each flip flop with bits moving LSB to MSB flip flop in each clock pulse, except the LSB flip flop whose input is output of XOR of N/2 and N flip flop. Thus single XOR operation is performed in each clock.XOR gate is permanently connected to the respective flip-flops of polynomial

$$F(X) = 1 + X^{N/2} + X^{N}$$

The circuit diagram of proposed N bit parallel LFSR having polynomial 1+ X3 + X6 is shown in fig 6.

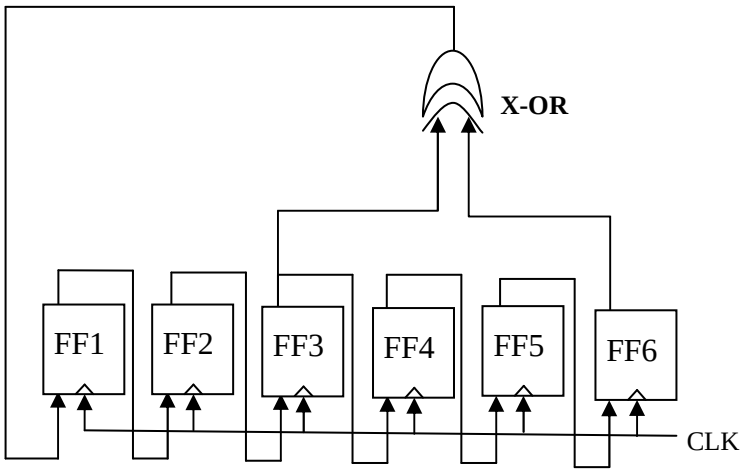


Figure 6 Output realization of F(X) = 1+ X3 + X6.

Let us consider the polynomial for N=6, F(X) = 1+ X3 + X6. Table 4 shows the storing procedure in order to obtain the parallel implementation. In cycle 1, XOR result of flip-flops 3 and 6 (which is calculated in the previous cycle) is stored in flip-flop 1. Similarly in clock cycle 2, 3, 4, 5, and 6 XOR results of flip- flops (2,5);

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

(1,4); (updated FF 1,3); (updated FF 2,2); and (updated FF 3,1) should be stored in flip- flop 3,4,5 and 6 respectively. The operation can be summarized as shown in Table 4.

Table 4 Update of flip-flops, F(X) = 1+ X3 + X6

| **Clock cycle** | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| **XOR result of** | 6,3 | 5,2 | 4,1 | 3, updated FF 1 | 2, updated FF 2 | 1, updated FF 3 |
| **Stored at FF** | 1 | 2 | 3 | 4 | 5 | 6 |

From table 2 and 4 it is found that the values updated at flip flop is same except the order in which they are stored in our design the values are stored in flip flop 1,2,3,4,5,6 respectively whereas in Abdullah Mamun and Rajendra Katti architecture[3] values are stored in flip flop 6,5,4,3,2,1 respectively.

### *2.2. N bit parallel Counter*

The name counter is used for any clocked sequential circuit whose state diagram contains a single cycle, as shown in fig 7. The modulus of a counter is the number of states in the cycle. A counter with m states is also called a modulo-m counter or sometimes, a divide-by-m counter. A counter whose modulus is not a power of 2 will, of necessity contains extra states that are not used in normal operation.

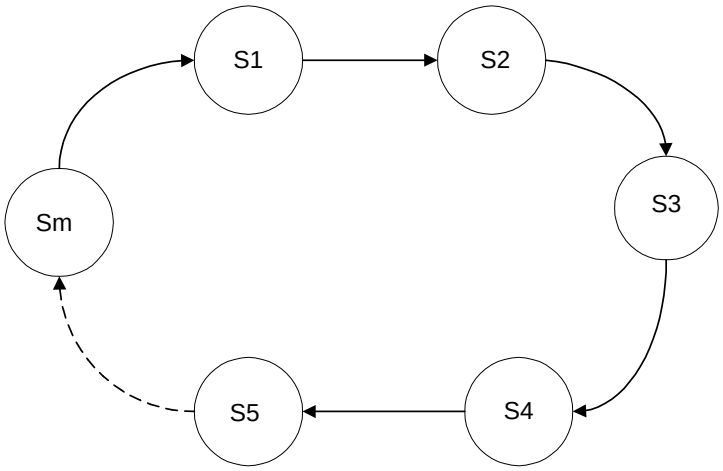


Figure 7 state diagram of counter.

The most commonly used counter type is N-bit binary counter. Such a counter has n flip-flops and has $2^N$ states, which are visited in the sequence 0, 1, and 2…. $2^N$-1, 0, 1. Each of the foregoing states is encoded in the corresponding N-bit binary integer.

## 3. IMPLEMENTATION AND RESULT

The complete experimental work start with the proposed design is modeled in Verilog [7]-[10]. Functional simulation, schematic generation, RTL generation, synthesis for hardware platforms in FPGA Vertex 5 series (xc5vlx30-3-ff324) target device was done of the design using Xilinx ISE Design Suite 9.2i.The proposed design is modeled in Verilog having synchronous reset, using input clk; input reset; input loadseed_i; input [31:0] seed_i; output [31:0] number_o; Several design methods are available for designing synchronous sequential circuits, Since the D flip-flop is an essential part of the FPGA, and we will focus on the behavioral modeling which is well suited for D flip-flops. The general form of the state equation for a D flip-flop is:

$$Q(t + 1) = D.$$

So the input for each D flip-flop is simply determined by finding an expression for the next state for that flip-flop.

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

### *3.1. SYNTHESIS*

The RTL Schematic and Technology Schematic of Advance parallel LFSR is shown in fig 8. HDL Synthesis of Advance parallel LFSR generated by Xilinx ISE Design Suite 9.2i is given below.

```
Synthesizing Unit <Advance_LFSR>.
    Related source file is "advace_LFSR.v".
    Found 32-bit register for signal <number_o>.
    Found 32-bit up counter for signal <Count_reg>.
    Found 32-bit register for signal <LFSR_reg>.
    Found 1-bit xor2 for signal <LFSR_reg$xor0000> created at line 132.
    Found 32-bit xor2 for signal <number_o$xor0000> created at line 156.
    Summary:
                                        inferred   1 Counter(s).
                                        inferred  64 D-type flip-flop(s).
Unit <Advance_LFSR> synthesized.

Advanced HDL Synthesis Report

Macro Statistics
# Counters                      : 1
 32-bit up counter              : 1
# Registers                     : 64
 Flip-Flops                    : 64
# Xors                          : 2
 1-bit xor2                    : 1
 32-bit xor2                   : 1
```

The device utilization summary is shown in table 5. The device utilization summary showed that minimum resources were consumed.

Table 5 SYNTHESIS RESULTS FOR VIRTEX SERIES DEVICES

| **Device Utilization parameter** | **Vertex 5 (Target device xc5vlx30-3-ff324,Package ff1676,Speed -1)** | |
|---|---|---|
| **Logic Utilization** | **Used** | **Utilization** |
| Number of Slices Registers | 96 Out of 19200 | 0% |
| Number of Slice LUTs | 98 Out of 19200 | 0% |
| Number of fully used LUT-FF pairs | 96 Out of 98 | 97% |
| Number of bonded IOBs | 67 Out of 220 | 30% |
| Number of BUFG/BUFGCTRLs | 1 Out of 32 | 3% |

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

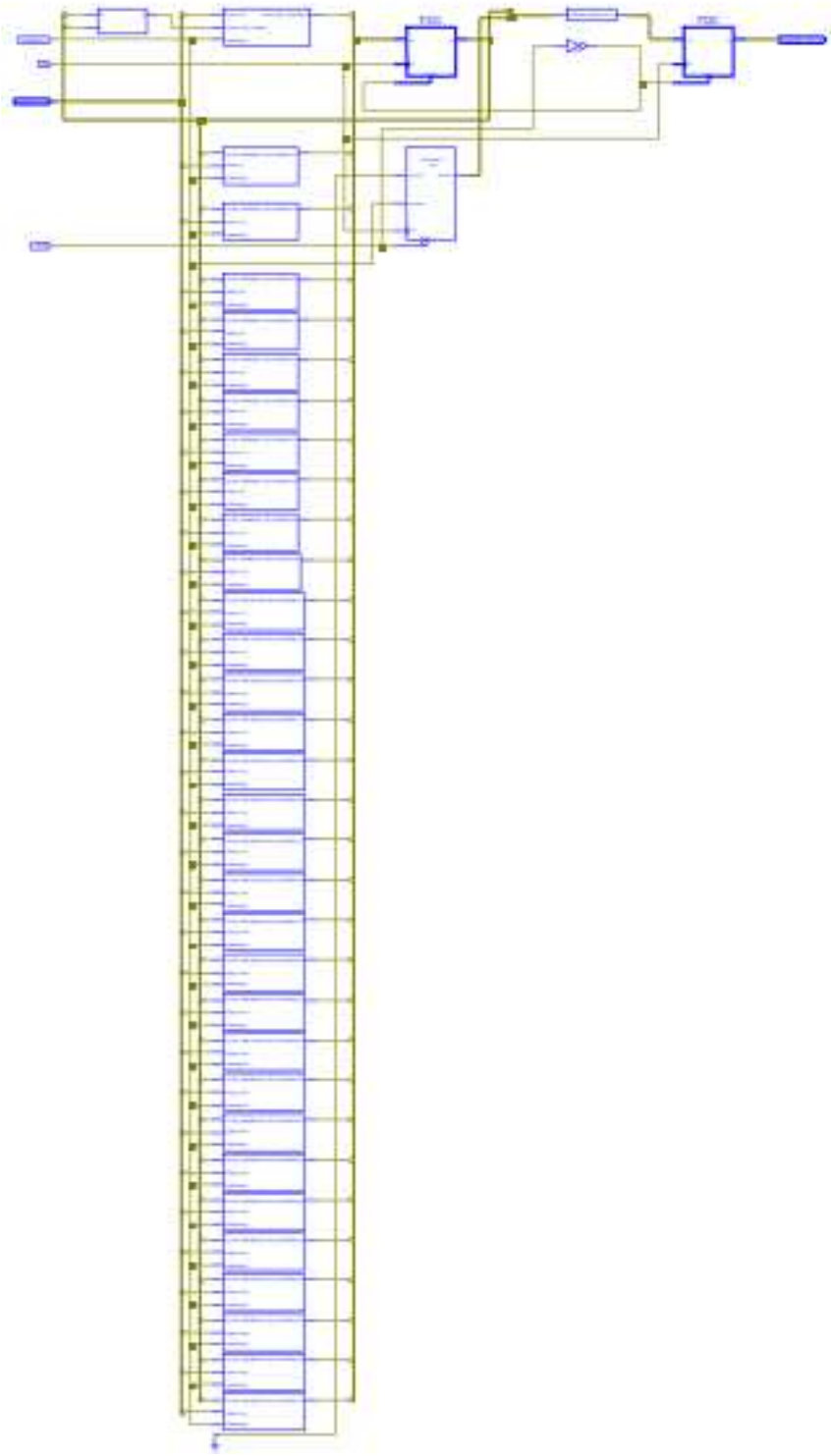

Figure 8 RTL Schematic of Advance parallel LFSR

### *3.2. SIMULATION TIMING WAVEFORM*

Timing simulation waveform of Advance parallel LFSR is shown in Fig. 9.

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

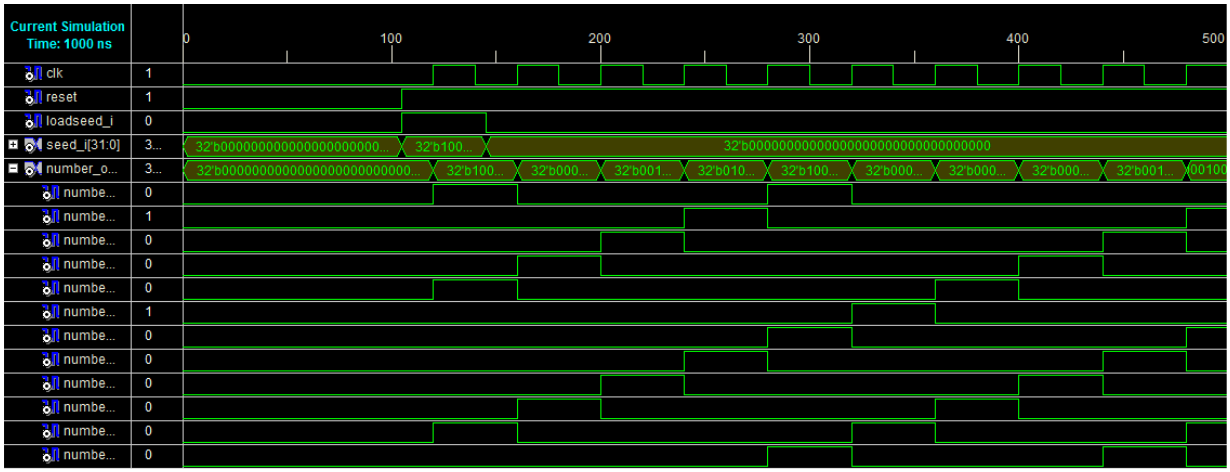


Figure 9 Simulation waveform of Advance parallel LFSR

## 4. CONCLUSION

In M. Lowy[1] and M. E. Hamid and C. I. H. Chen[2] [4] design , 2 output of 1 bit can be obtained in a single clock cycle with increase in number of switches and in Abdullah Mamun and Rajendra Katti[3] [4] 2 output of N/2 bit can be obtained in a single clock cycle with reduce dynamic power consumption.

The proposed advance N bit parallel LFSR has at least $2^N$ random states because the N bit parallel counter has $2^N$ states and is formed by XOR with N-bit parallel LFSR having polynomial 1+ X16 + X32 but at a increased number of hardware the synthesis results for Virtex series devices shows 96 flip flop are used as given in table 5.2. Total memory usage is 289604 kilobytes which is very low.Hence it can be used in cryptography where low memory utilization and high level of security is required. The device utilization summary showed that minimum resources were consumed.

## References

[1] M. Lowy,(1996) “Parallel implementation of linear feedback shift registers for low power applications,” IEEE Trans. Circuits Syst. II, vol. 43, pp. 458–466, June 1996.
[2] Hamid, Muhammad E.; Chen, Chien-In Henry, (1998)“Note to low- power linear feedback shift registers,” IEEE Trans. on Circuits and Systems II: Analog and Digital Signal Processing, vol. 45, Issue 9, pp 1304-1307, September 1998.
[3] Abdullah Mamun and Rajendra Katti(1998). “A new parallel architecture for low power linear feedback shift registers” IEEE Transactions on Circuits and Systems—II: ANALOG AND DIGITAL SIGNAL PROCESSING, VOL. 45, No. 9, September 1998.
[4] Shilesh Malliyoor and Chao You (2007)“Comparison of hardware implementation and power consumption of low-power multiple output linear feedback shifts register” journal of engineering, computing and architecture. Volume 1, Issue 1, 2007.
[5] Knut Wold(2011) “Security Properties of a Class of True Random Number Generators in Programmable Logic” Thesis submitted to Gjøvik University College for the degree of Doctor of Philosophy in Information Security.
[6] Mishra Shiv dutta, Shrivastav Anurag,(2013) “Design and Analysis of FPGA based cryptographic N-bit parallel LFSR” International journal of latest trends in Engineering and Technology, nov 2013
[7] Xilinx website *http://www.xilinx.com.*
[8] Bhasker J, (2006) “A VHDL Primer”, P T R Prentice Hall, Pages 1-2, 4-13, 28-30.
[9] Stephen Brown, Zvonko Vranesic (2007) ”fundamental of Digital logic with Verilog design”,2e, Tata McGraw-Hill,Delhi,2007.
[10] Field programmable gate array (2012). Wikipedia website. Online Available: *http ://en.wikipedia.org /wiki/ Field-programmable_gate_array.*