A High Performance Realization of 8 Bit Reversible LFSR Encryption And Decryption

T Madhu[1], A. Suresh Babu[2], Vidadala Srija[3]
[1] Dept of ECE
[2, 3]Asst. Professor, Dept of ECE
[1, 2] Swetha Institute of Technology & Science, Tirupathi, Andhra Pradesh-517561
[3]St.Martin's Engineering College, Dhulapally, Secunderabad, Telangana-500100

Abstract- *This Paper presents a novel architecture of pulse triggered and edge triggered SISO & SIPO registers. We are going to analyze their quantum cost, delay and garbage in terms of some lemmas. We will explain with an example of sequence pulse generation with minimized delay & cost by using registers. In this paper we are going to realize a reversible architecture of LFSR and PSA which can be used for random bit generation.*

Keywords- LFSR, PSA, Encryption, Decryption, Reversible, VHDL.

I. INTRODUCTION

The concept of a reversible memory cell was first shown by Fredkin and Toffoli, in 1982, where, design of a JK latch was introduced. Later, in 1996, Picton developed a design of clock less SR-latch using two cross coupled NOR gate, where NOR gates were designed from Fredkin gate. All the reversible latches such as D-Latch, T-latch etc. along with their flip-flop and master-slave configuration were introduced for the first time in 2005 by Thapliyal in 2006, Rice introduced a SR-latch without fan-out problem available in the design by Picton and subsequently designed other latches from SR. In 2007, Thapliyal and Vinod existed a better design of reversible flip-flops than by Rice in terms of number of reversible gates being used and garbage outputs. In this section we are discussing about some previous existing systems regarding to LFSR.

Latika Desai and Suresh Mali [1] presented system is highly secured due to its successful implementation in hardware. By using cache memory, they did encryption of CI, the random addresses of cache memory are used for scribbling CI to be embedded in the cover bit by bit fashion. One cannot extract CI unless he/she knows the algorithm and look-up table as a key of embedding. Pipelining process while embedding enhances the speed of embedding and optimizes the memory utilization.

Jayasanthi M, Kowsalyadevi AK [2] provides new low power architecture for Linear Feedback Shift Register. They replaced pulsed D latches with D flip-flop with clock pulses. The power consumption and delay of the circuit got reduced. This pattern generation by LFSR can also be used in data encryption circuits to provide security for generation of binary sequence. It is also used in retrieving the data after recombination and reception.

Jerome Burke John McDonald Todd Austin [3] examines their performance on micro architecture models of varying cost and performance. Performance analysis of the optimized benchmarks revealed a 59% speedup over machines with rotate instructions, and a 74% speedup over machines without rotates.

M. B. Abdelhalim, M. El-Mahallawy, A. Elhennawy [4] a hardware implementation of the Modified TEA algorithm (MTEA) is proposed which uses the Linear Feedback Shift Register (LFSR) to overcome the security weakness of the standard TEA algorithm against attacks. The implementation of MTEA algorithm is benchmarked with the standard TEA algorithm considering the area, throughput and power consumption.

Shailaja A., Krishnamurthy G.N [5] the performance of the RC7-RLGC architecture was analyzed in the FPGA platform over high configurable Vertex devices such as Virtex-6, LP- Virtex-6 and Virtex-7. The RC7-RLGC architecture obtained strong security by incorporating randomized key generation RLG circuit. The proposed algorithm occupied less FPGA device utilization on LP-Virtex-6 device; 13.04 % of LUTs, 10 % of flip-flops and 36.363 % of slices than existing RC7 algorithm.

II. IMPLEMENTATION OF PROPSED REVERSIBLE LFSR

Linear Feedback Shift Register (LFSR) is used to generate periodic sequence, but it does not produce all zero sequence until it starts from all zero. A LFSR can be constructed by doing exclusive-OR on the outputs of two or more of the FFs together and applying this output to one of the FFs. The Fig.1 shows the design of 4 bit reversible LFSR.

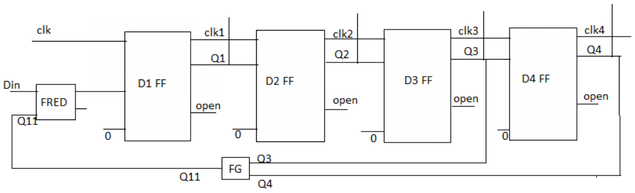


Fig.1 proposed 4 bit Reversible LFSR

III. PROPOSED ARCHITECTURE USING REVERSIBLE LFSR FOR IMAGE ENCRYPTION AND DECRYPTION

Theproposed architecture consists of Altera memory blocks and two four bit reversible LFSR connected as show in Fig.2. Initially the memory loaded with 64 pixels' data which is to be the data in for 8 bit LFSR. Each pixel 8-bit data can be divided into two 4-bit data and then given to two 4 bit reversible LFSR to convert encrypted data which is shown in Fig.3.This encrypted data stored into Altera memory.

This encrypted 8-bit data again is given to two 4 bit reversible LFSR it will give back the original image pixel values as shown in Fig.3. For example, LFSR loaded with a seed value is "1100(12)" after eight iterations it will generate a pseudorandom pattern of "1111(15)" again if it is given back to same LFSR after eight iterations it will generate a pseudorandom pattern of "1100". The sequences of iterations are 1100,0110,1011,0101,1010,1101,1110,1111 for encrypted vales.

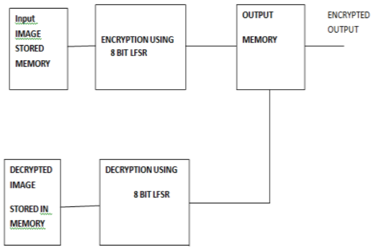
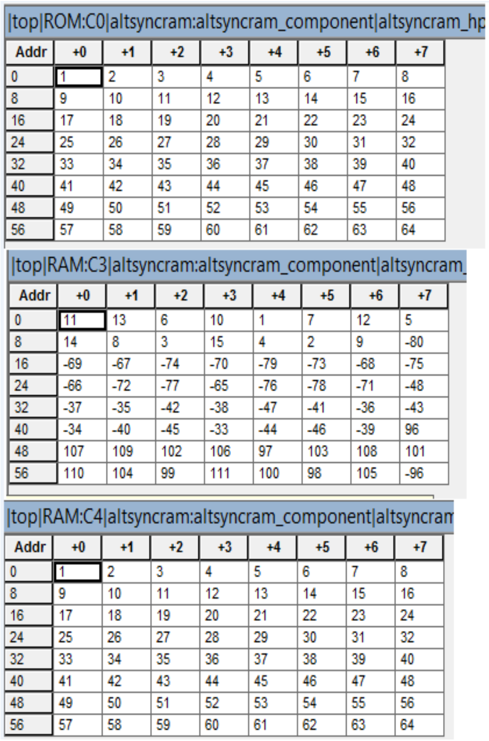


Fig.4 Realization of Reversible LFSR for encryption and decryption



|top|ROM:C0|altsyncram:altsyncram_component|altsyncram_hp

Addr	+0	+1	+2	+3	+4	+5	+6	+7
0	1	2	3	4	5	6	7	8
8	9	10	11	12	13	14	15	16
16	17	18	19	20	21	22	23	24
24	25	26	27	28	29	30	31	32
32	33	34	35	36	37	38	39	40
40	41	42	43	44	45	46	47	48
48	49	50	51	52	53	54	55	56
56	57	58	59	60	61	62	63	64

|top|RAM:C3|altsyncram:altsyncram_component|altsyncram_

Addr	+0	+1	+2	+3	+4	+5	+6	+7
0	11	13	6	10	1	7	12	5
8	14	8	3	15	4	2	9	-80
16	-69	-67	-74	-70	-79	-73	-68	-75
24	-66	-72	-77	-65	-76	-78	-71	-48
32	-37	-35	-42	-38	-47	-41	-36	-43
40	-34	-40	-45	-33	-44	-46	-39	96
48	107	109	102	106	97	103	108	101
56	110	104	99	111	100	98	105	-96

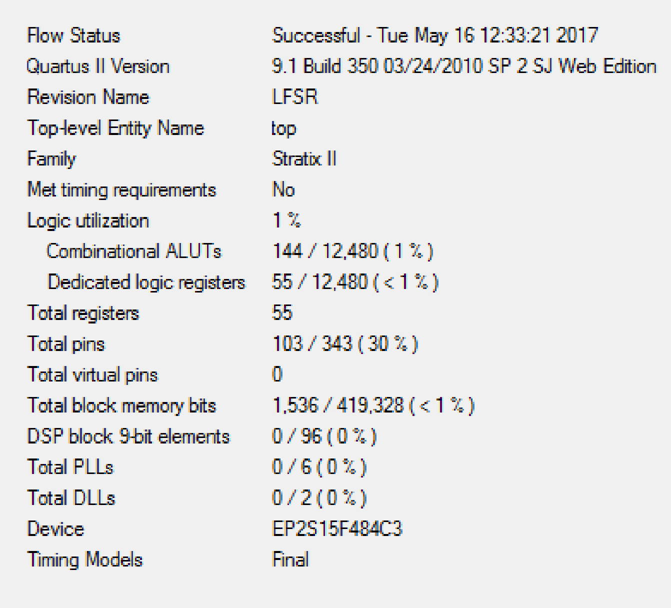
|top|RAM:C4|altsyncram:altsyncram_component|altsyncram

Addr	+0	+1	+2	+3	+4	+5	+6	+7
0	1	2	3	4	5	6	7	8
8	9	10	11	12	13	14	15	16
16	17	18	19	20	21	22	23	24
24	25	26	27	28	29	30	31	32
32	33	34	35	36	37	38	39	40
40	41	42	43	44	45	46	47	48
48	49	50	51	52	53	54	55	56
56	57	58	59	60	61	62	63	64

Fig.3 memory with input data, encrypted and decrypted data

IV. RESULTS AND DISCUSSIONS

In this section we are discussing about results of the proposed system. The below Fig.4 shows that Design summary for proposed top 8 bit reversible LFSR for image encryption. 8 bit reversible LFSR is implemented in one of the FPGA Family is QUARTUS II version and StratixII family. The above 8 bit reversible LFSR takes 144 combinational ALUTs,55 dedicated logic registers and totally 103 Input and output pins to functioning the 8 bit reversible LFSR.The above 8 bit reversible LFSRtakes <1% logic utilization with device used is EP2S15F484C3 and this design has been used 1,536 memory bits and zero DSP elements



Flow Status	Successful - Tue May 16 12:33:21 2017
Quartus II Version	9.1 Build 350 03/24/2010 SP 2 SJ Web Edition
Revision Name	LFSR
Top-level Entity Name	top
Family	Stratix II
Met timing requirements	No
Logic utilization	1 %
Combinational ALUTs	144 / 12,480 (1 %)
Dedicated logic registers	55 / 12,480 (< 1 %)
Total registers	55
Total pins	103 / 343 (30 %)
Total virtual pins	0
Total block memory bits	1,536 / 419,328 (< 1 %)
DSP block 9-bit elements	0 / 96 (0 %)
Total PLLs	0 / 6 (0 %)
Total DLLs	0 / 2 (0 %)
Device	EP2S15F484C3
Timing Models	Final

Fig.4 Design summary for proposed top 8 bit reversible LFSR for image encryption

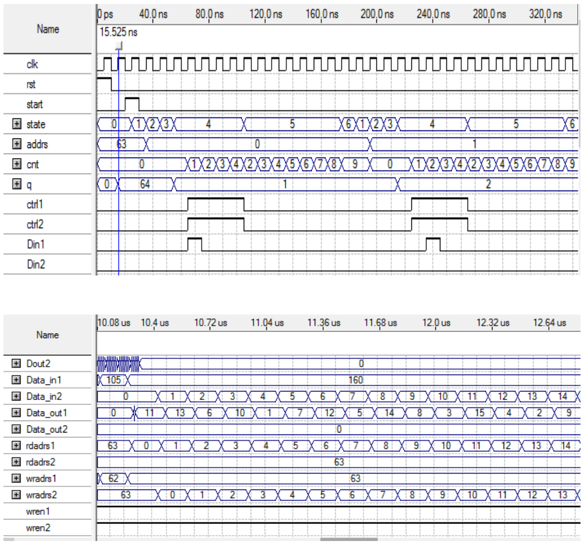


Fig.5 Simulation results for proposed 8 bit reversible LFSR for image encryption

The above Fig.5 is the representation of simulation results for proposed 8 bit reversible LFSR for image encryption.8 bit reversible LFSR is implemented in one of the FPGA Family is QUARTUS II version and Stratix II family. The below Fig.6 shows that RTL Schematic for top module Reversible LFSR for encryption and decryption

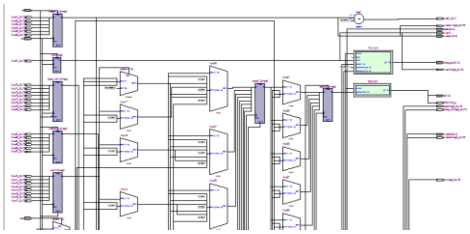
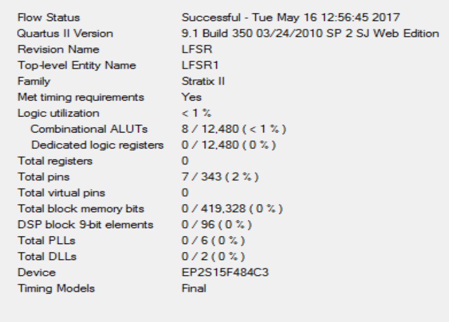


Fig.6 Schematic for top module Reversible LFSR for encryption and decryption



Flow Status	Successful - Tue May 16 12:56:45 2017
Quartus II Version	9.1 Build 350 03/24/2010 SP 2 SJ Web Edition
Revision Name	LFSR
Top-level Entity Name	LFSR1
Family	Stratix II
Met timing requirements	Yes
Logic utilization	< 1 %
Combinational ALUTs	8 / 12,480 (< 1 %)
Dedicated logic registers	0 / 12,480 (0 %)
Total registers	0
Total pins	7 / 343 (2 %)
Total virtual pins	0
Total block memory bits	0 / 419,328 (0 %)
DSP block 9-bit elements	0 / 96 (0 %)
Total PLLs	0 / 6 (0 %)
Total DLLs	0 / 2 (0 %)
Device	EP2S15F484C3
Timing Models	Final

Fig.7 Design summary for proposed 4 bit reversible LFSR

The above Fig.7 is the representation of design summary for proposed 4 bit reversible LFSR .8 bit reversible LFSR is implemented in one of the FPGA Family is QUARTUS II version and StratixII family. The above 8 bit reversible LFSR takes 8 combinational ALUTs and totally 7 Input and output pins to functioning the 4 bit reversible LFSR. Fig.8shows that Simulation results for proposed 4 bit reversible LFSR

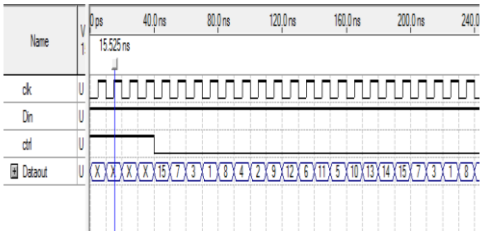


Fig.8 Simulation results for proposed 4 bit reversible LFSR

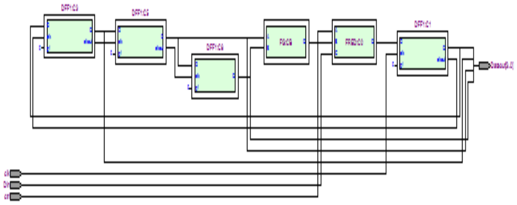


Fig.9 RTL Schematic for 4 bit reversible LFSR

The above Fig.9 shows that RTL Schematic for 4 bit reversible LFSR

V. CONCLUSION

Due to the feedback function, a LFSR can produce a sequence of random bits which has a very long cycle. Therepeating sequence of bit patterns of an LFSR allows it to be used as a frequency divider or as a counter when a non-binary pattern is acceptable. In this paper, we have demonstrated novel architecture of pulse triggered and edge triggered SISO & SIPO registers and analyzed their quantum cost, delay and garbage in terms of some lemmas. Usingthe registers, we have shown an example of sequence pulse generation with minimized delay & cost. Lastly, we have realized reversible architecture of LFSR and PSA which can be used for random bit generation.

REFERENCES

[1] Latika Desai and SureshMali, “Crypto-Stego-Real-Time (CSRT) System forSecure Reversible Data Hiding”, HindawiVLSI DesignVolume 2018, Article ID 48047297.

[2] Jayasanthi M, Kowsalyadevi AK, “Low Power Implementation of Linear Feedback Shift Registers”,International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-2, July 2019.

[3] Jerome Burke John McDonald Todd Austin, “Architectural Support for Fast Symmetric-Key Cryptography”.

[4] M. B. Abdelhalim, M. El-Mahallawy, A. Elhennawy, “Design and Implementation of an Encryption Algorithm for use inRFID System”, International Journal of RFID Security and Cryptography (IJRFIDSC), Volume 2, Issue 1, June 2013.

[5] Shailaja A., Krishnamurthy G.N, “FPGA Implementation and Analysis of RC7 Algorithm Using Reversible Logic Gates, “.International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6, August 2019.