Design and Analysis of Modified Dual-CLCG Algorithm for Pseudo Random Bit Generator

[1]Sayyada Zehra Khadija, [2]M.RamaKrishna
[1]M.Tech Scholar, Department of ECE, Jyothishmathi Institute of Technology and Science, Karimnagar, India
[2]Associate Professor, Department of ECE, Jyothishmathi Institute of Technology and Science, Karimnagar, India.

ABSTRACT:A pseudorandom bit generator (PRBG) is a crucial element in ensuring the security of data during its transmission and storage in different cryptographic applications. Out of the commonly used techniques for generating pseudorandom numbers, including linear feedback shift register (LFSR), linear congruential generator (LCG), connected LCG (CLCG), and dual-coupled LCG (dual-CLCG), the dual-CLCG approach is shown to be more safe. This approach utilizes in equality comparisons to generate pseudorandom bits at regular intervals. Therefore, a novel design of the dual-CLCG technique is created, which produces pseudo-random bits at a consistent clock rate. This work proposes a novel approach termed "modified dual-CLCG" for pseudo- random bit generation (PRBG) together with a very large-scale integration (VLSI) architecture. The purpose of this method is to address the aforementioned concerns. The innovative feature of the proposed PRBG approach is its ability to create pseudorandom bits at a consistent clock rate, with just one initial clock delay and little hardware complexity.

1. Introduction

Security and privacy over the internet is the most sensitive and primary objective to protect data in various ways. Pseudo-Random Bit Generators (PRBGs) play a fundamental role in various fields such as cryptography, simulation, and secure communication systems. They are essential for generating sequences of bits that exhibit characteristics of randomness, making them suitable for cryptographic keys, statistical simulations, and more. The quality and efficiency of a PRBG are paramount for ensuring the security and reliability of systems that relyonrandombitsequences.wepresentthedesignofaModifiedDual-CLCG(CombinedLinearCongruential Generator).

For IoT enabled hardware applications. The proposed PRBG method i.e. “modified dual-CLCG” and its VLSI architecture have the following advantages and novel contributions over previous PRBG method. First, a single XOR logic is utilized at the output stage for generating pseudorandom bit at uniform clock rate which leads to lower the hardware cost. Secondly, it generates a maximum length of 2^npseudo random bits with one initial clock latency. Third, the proposed modified dual-CLCG method passes all the fifteen bench mark tests of NIST standard and is proved to be polynomial-time unpredictable. The randomness tests are performed using NIST test tool sts-2.1.2. Further, the properties of the proposed PRBG method are investigated theoretically by using the probabilistic approach. It shows that the proposed modified dual-CLCG system has the Similar security strength of dual CLCG method and the probabilistic algorithm to obtain the initial seed requires the solution of n2^4.The architecture of the existing dual-CLCG method and the proposed modified dual-CLCG method for different word size of n8 was implemented using Verilog HDL.

This paper is organized as follows: architectural mapping of the existing dual-CLCG method is performed and The proposed PRBG method along with its randomness properties are discussed .he efficient VLSI architecture of the proposed modified dual-CLCG method.

Combined linear congruential generators, as the name implies, are a type of PRNG (pseudorandom number generator) that combine two or more LCGs (linear congruential generators). The combination of two or more LCGs into one random number generator can result in a marked increase in the period length of the generator which makes them better suited for simulating more complex systems. The combined linear congruential generator algorithm is defined as:

$$X_i \equiv (\sum^{k}(-1)^{J-1}Y_{ij})(\mathrm{mod}(m1-1))\ j=1$$

Where m1m1 is the modulus of the LCG, Yi,j Yi,j is the iith input from the jjth LCG and Xi Xi is the iith random generated value. L'Ecuyer describes a combined linear generator that utilizes two LCGs in Efficient and Portable Combined Random Number Generators for32-bit processors. Algorithm for a PRBG. The objective of this modification is to improve the efficiency and statistical properties of the generated random bit sequences. The Dual- CLCG algorithm combines the outputs of two Linear Congruential Generators(LCGs) with distinct seeds to produce random bits. Linear Congruential Generators are a common choice for generating pseudo-random sequences due to their simplicity and speed. However, their periodicity and statistical properties can be limited when used individually. The Dual-CLCG algorithm overcomes these limitations by leveraging the combined powerof two LCGs while carefully selecting seed values and parameters.

Modified Dual CLCG

Modified algorithm of dual-coupled linear congruential generator (dual-CLCG) for pseudo-random bit generation is proposed to achieve the high randomness properties of generated bit sequence with minimum VLSI complexity. The proposed method relies based on randomly chosen inequality comparisons bits by the multiplexer circuit and its select line is control by current seeds value to generates final random bits. Therefore, a new method for random bit generator i.e. modified dual-CLCG and its VLSI architecture are proposed in this work to mitigate the more secure random bit generator. The effect of modification on the design of a dual CLCG is observed to evaluate the some of the essential timing performance parameters such as initial clock latency, maximum possible frequency of bit generation and output –to-output latency. Also find the power dissipation and utilize chip area. The proposed architecture with 8, 16 and 32-bit length is design using Verilog-HDL and its synthesis is done based on 90-nm CMOS technology (GPDK) using Cadence Tool

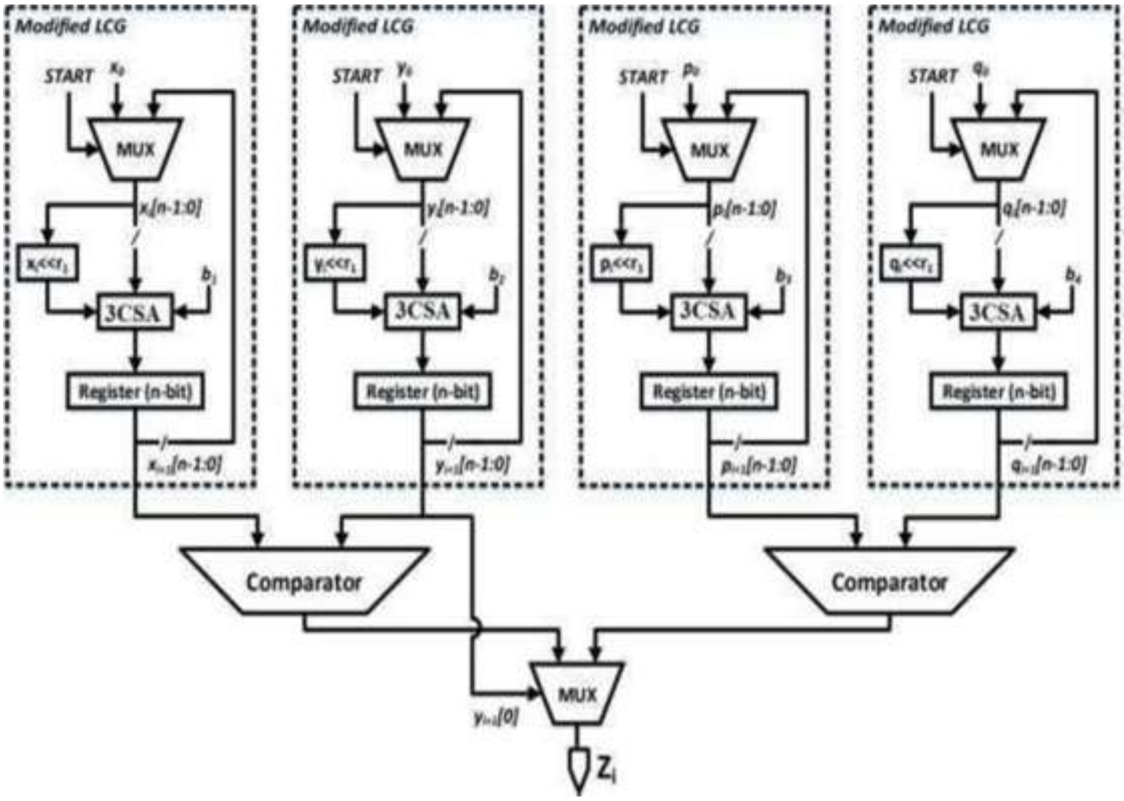


Fig.1Modified Dual CLCG

A block diagram of a Modified Dual CLCG (Complementary Linear Congruential Generator) structure typically consists of four linear congruential generators (LCGs) operating in parallel, with additional components for combining their outputs. Here's a breakdown of the components and their functions:

LCG1: This is the first linear congruential generator in the structure. It generates a sequence of pseudo-random numbers using a linear recurrence relation of the form Combiner: This component combines the outputs of LCG1 and LCG2 to generate the final sequence of pseudo- random numbers. There are different methods for combining the outputs, such as adding, subtracting, XOR ing, or using other mathematical operations. The purpose of combining the outputs is to enhance the statistical properties of the generated random numbers.

Output: This is the final output of the Modified Dual CLCG structure, consisting of a sequence of pseudo- random numbers with improved randomness properties compared to using a single linear congruential generator.

The dual-CLCG algorithm for pseudorandom bit generator was proposed in. It is a dual coupling of four LCG block and it is given by following recurrence equations:

$$x_{i+1} = [(2^{r1} \times x_i) + x_i + b_1] mod 2^n \qquad (1)$$

$$y_{i+1} = [(2^{r2} \times y_i) + y_i + b_2] mod 2^n \qquad (2)$$

$$p_{i+1} = [(2^{r3} \times p_i) + p_i + b_3] mod 2^n \qquad (3)$$

$$q_{i+1} = [(2^{r4} \times q_i) + q_i + b_4] mod 2^n \qquad (4)$$

$$B_i = \begin{Bmatrix} 1 \; if \; x_{i+1} > y_{i+1} \\ 0 \; if \; x_{i+1} < y_{i+1} \end{Bmatrix} \qquad (5)$$

$$C_i = \begin{Bmatrix} 1 \; if \; p_{i+1} > q_{i+1} \\ 0 \; if \; p_{i+1} < q_{i+1} \end{Bmatrix} \qquad (6)$$

$$z_i = B_i{}^\wedge C_i \qquad (7)$$

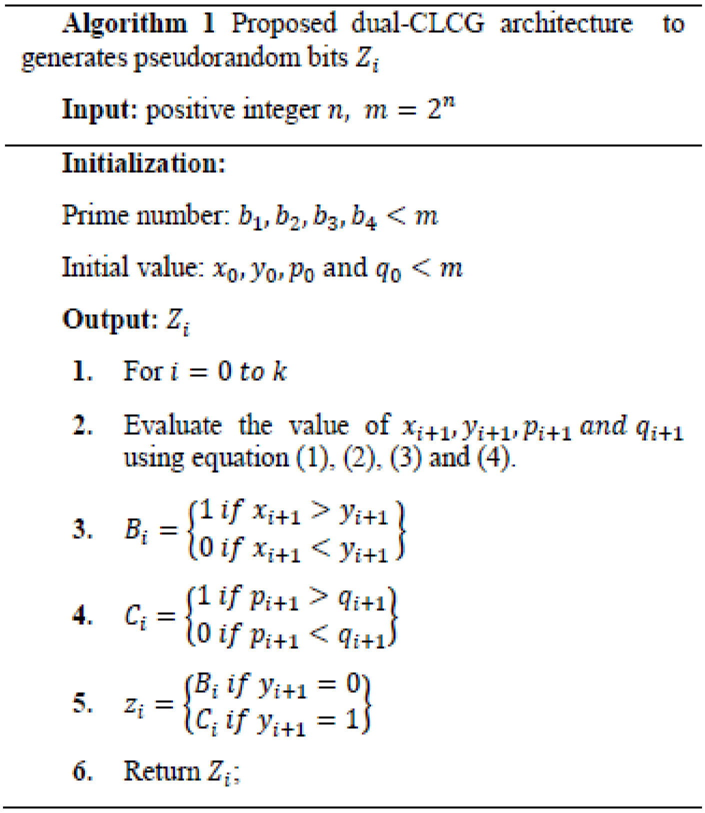
Here the constant parameter and initial seeds value for above recurrence equations. Here shifting value is the positive integer i.e. The final output of random bit sequence is given by variable. It is evaluated based on Equations (5) to (6) in each iteration. To enhance the randomness properties of the random sequence, we can modify the equation (7) and it is relies based on randomly chosen in equality comparisons bits by the multiplexer circuit and its select line is control by current seeds value [1] to generates final random bit sequence i.e. given by equation(8).

$$z_i = \begin{Bmatrix} B_i \; if \; y_{i+1} = 0 \\ C_i \; if \; y_{i+1} = 1 \end{Bmatrix} \qquad (8)$$

LCG1 and LCG 2 operate independently in parallel, each generating its own sequence of pseudo- random numbers. The parameters (multipliers, increments, and module) of LCG 1 and LCG 2 are carefully chosen to ensure they are statistically independent and have long periods.

The outputs of LCG 1 and LCG 2 are combined using the combiner component. This combination can involve various mathematical operations that help reduce correlations between successive random numbers and improve the overall randomness of the sequence. The combined output from the combiner forms the final sequence of pseudo-random numbers, which can be used in various applications requiring random number generation.

LCG2: This is the second linear congruential generator in the structure. It also generates a sequence of pseudo- random numbers but uses different parameters compared to LCG 1.Overall, the Modified Dual CLCG structure enhances the quality of random number generation by leverageing two complementary linear congruential generators and combining their outputs to produce a sequence with improved statistical properties.



```
Algorithm 1 Proposed dual-CLCG architecture to generates pseudorandom bits $Z_i$
Input: positive integer $n$, $m = 2^n$
Initialization:
Prime number: $b_1, b_2, b_3, b_4 < m$
Initial value: $x_0, y_0, p_0$ and $q_0 < m$
Output: $Z_i$
1. For $i = 0\ to\ k$
2. Evaluate the value of $x_{i+1}, y_{i+1}, p_{i+1}\ and\ q_{i+1}$ using equation (1), (2), (3) and (4).
3. $B_i = \begin{Bmatrix} 1\ if\ x_{i+1} > y_{i+1} \\ 0\ if\ x_{i+1} < y_{i+1} \end{Bmatrix}$
4. $C_i = \begin{Bmatrix} 1\ if\ p_{i+1} > q_{i+1} \\ 0\ if\ p_{i+1} < q_{i+1} \end{Bmatrix}$
5. $z_i = \begin{Bmatrix} B_i\ if\ y_{i+1} = 0 \\ C_i\ if\ y_{i+1} = 1 \end{Bmatrix}$
6. Return $Z_i$;
```

Results and Analysis

The RTL schematic is abbreviated as the register transfer level it denotes the blue print of the architecture and is used to verify the designed architecture to the ideal architecture that we are in need of development. The hdl language is used to convert the description or summery of the architecture to the working summery by use of the coding language i.e verilog ,VHDL. The RTL schematic even specifies the internal connection blocks for better analyzing. The figure 6.1 represented below shows the RTL schematic diagram of the designed architecture.

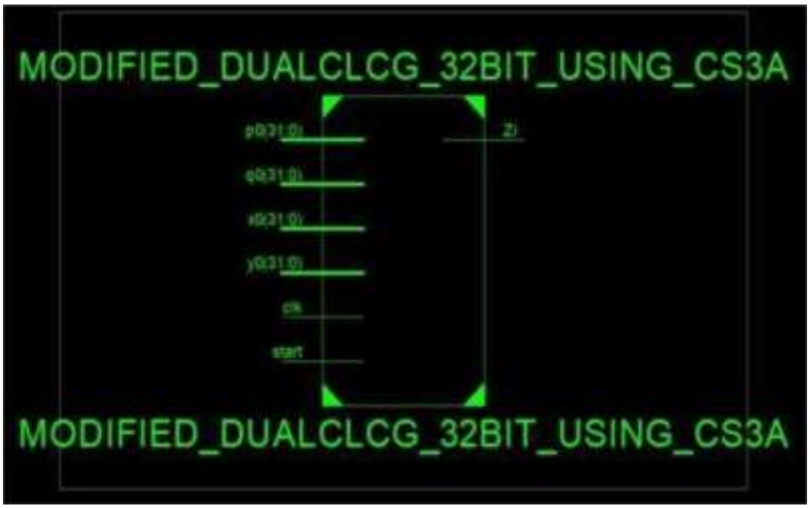

MODIFIED_DUALCLCG_32BIT_USING_CS3A
p0(31:0)
q0(31:0)
x0(31:0)
y0(31:0)
clk
start
Zi
MODIFIED_DUALCLCG_32BIT_USING_CS3A

Fig.2RTLSchematic view of Modified Dual CLCG using CS3A

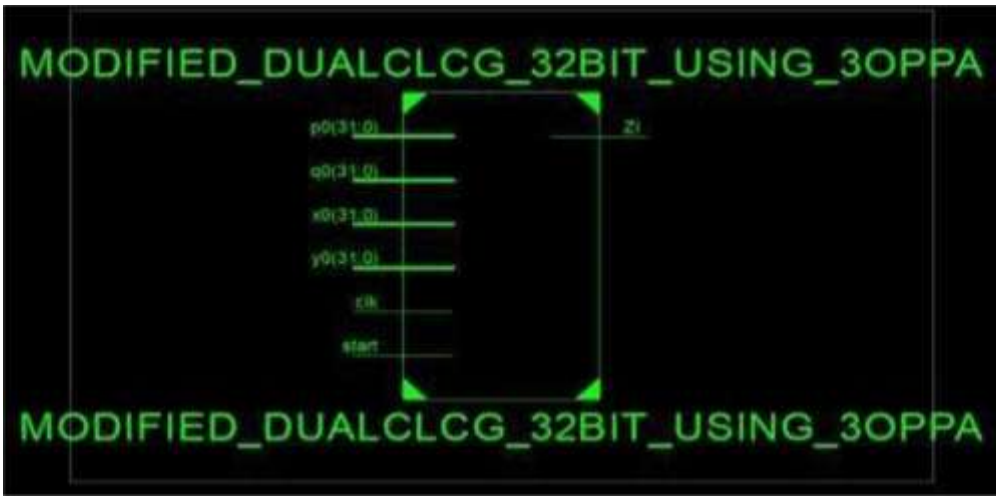

MODIFIED_DUALCLCG_32BIT_USING_3OPPA
p0(31:0)
q0(31:0)
x0(31:0)
y0(31:0)
clk
start
Zi
MODIFIED_DUALCLCG_32BIT_USING_3OPPA

Fig.3.RTLSchematic view of proposed Modified Dual CLCG using three operand Adder

Technology schematic

The technology schematic makes the representation of the architecture in the LUT format ,where the LUT is consider as the parameter of are a that is used in VLSI to estimate the architecture design. The LUT is consider as an square unit the memory allocation of the code is represented in there LUT s in FPGA.

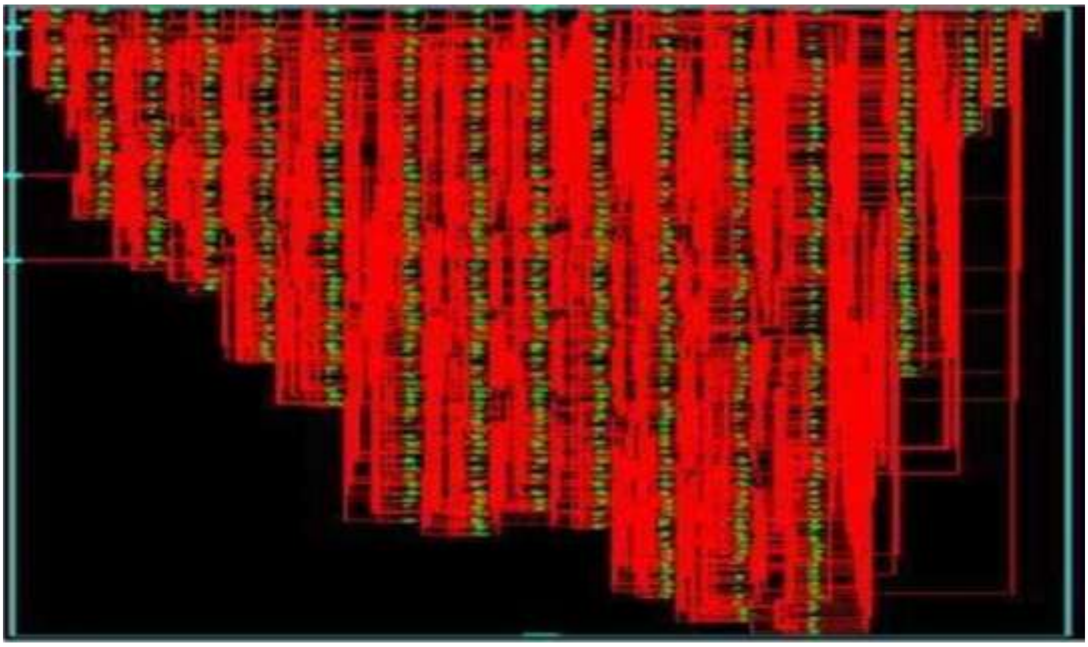


Fig.4 View technology Schematic of modified Dual CLCG using CS3A

Simulation

The simulation is the process which is termed as the final verification in respect to its working whereas the schematic is the verification of the connections and blocks. The simulation window is launched as shifting from implementation to the simulation on the home screen of the tool, and the simulation window confines the output in the form of wave forms output. Here it has the flexibility of providing the different radix number systems.

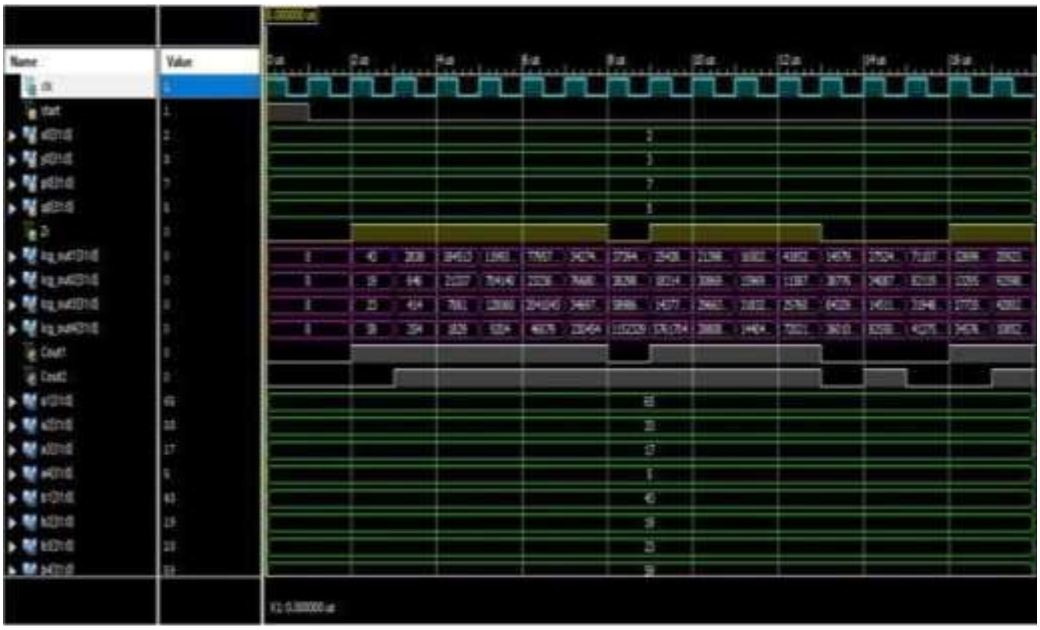


Fig.5 simulated wave form of modified Dual CLCGusingCS3A

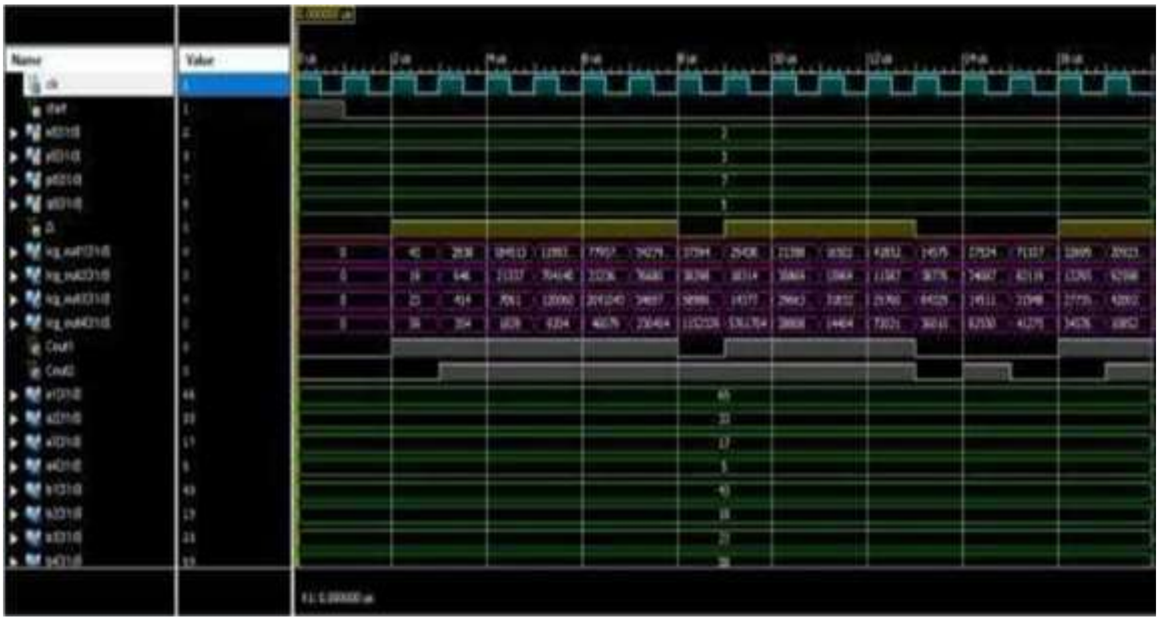
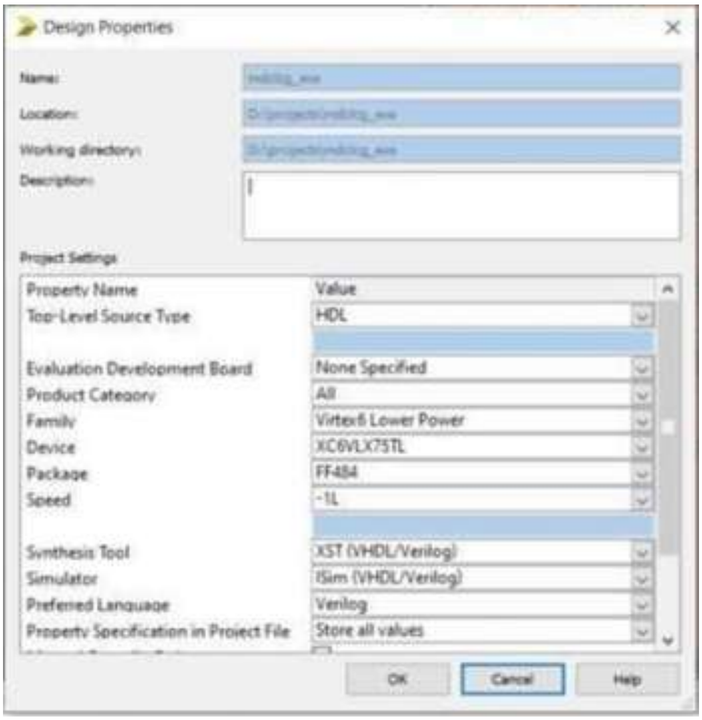


Fig 6 Simulated wave form of proposed modified Dual CLCG using three operand PPA



Design Properties

Name: mdclcg_ww

Location: D:\projects\mdclcg_ww

Working directory: D:\projects\mdclcg_ww

Description:

Project Settings

Property Name	Value
Top-Level Source Type	HDL
Evaluation Development Board	None Specified
Product Category	All
Family	Virtex6 Lower Power
Device	XC6VLX75TL
Package	FF484
Speed	-1L
Synthesis Tool	XST (VHDL/Verilog)
Simulator	ISim (VHDL/Verilog)
Preferred Language	Verilog
Property Specification in Project File	Store all values

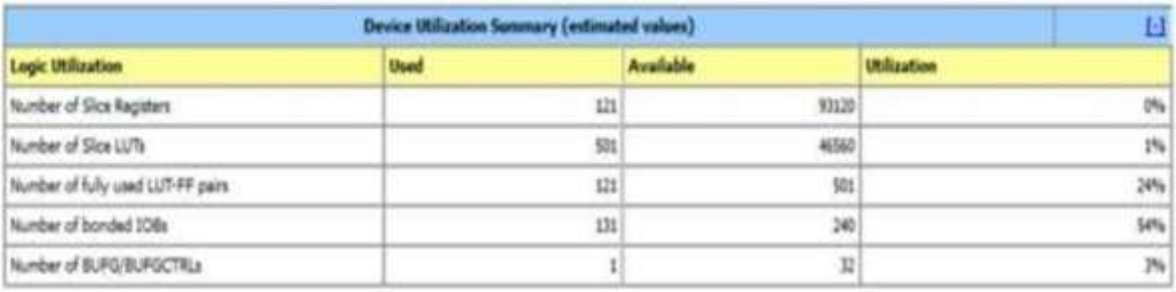
Fig.7. family selected for synthesis

Parameters

Consider in VLSI the parameters treated are area, delay, frequency and power, based on these parameters one canjudge the one architecture to other. Here the consideration of are a and power consumptions are considered the parameters are obtained by using the tool XILINX14.7and the HDL is verilog language. When frequency is more for any design it will increase the speed of design.

Parameter	Existed design	Proposed design
Frequency(MHz)	132.714	225.683

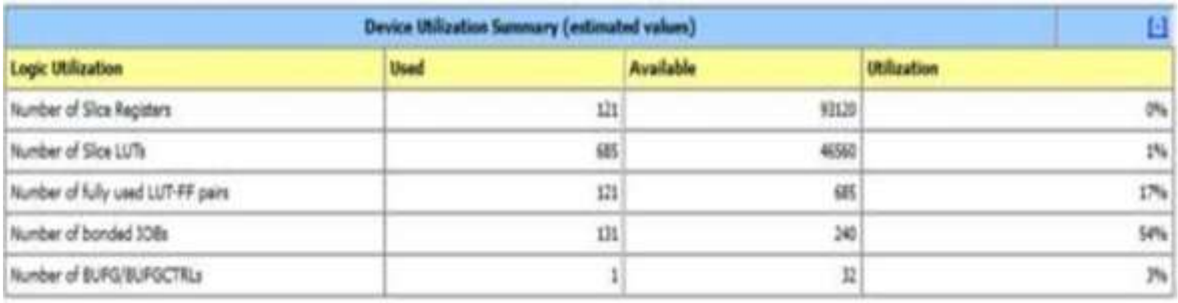
Table.1.ParameterComparison Existed Design Results



Device Utilization Summary (estimated values)			[-]
Logic Utilization	Used	Available	Utilization
Number of Slice Registers	121	93120	0%
Number of Slice LUTs	501	46560	1%
Number of fully used LUT-FF pairs	121	501	24%
Number of bonded IOBs	131	240	54%
Number of BUFG/BUFGCTRLs	1	32	3%

Table.2. Existed design results Minimum period:7.535ns(Maximum Frequency:132.714MHz)Minimum input arrival time before clock: 7.610ns Maximum output required time after clock:2.666ns

Proposed Design Results



Device Utilization Summary (estimated values)			[-]
Logic Utilization	Used	Available	Utilization
Number of Slice Registers	121	93120	0%
Number of Slice LUTs	685	46560	1%
Number of fully used LUT-FF pairs	121	685	17%
Number of bonded IOBs	131	240	54%
Number of BUFG/BUFGCTRLs	1	32	3%

Table.3Proposed Design Results Minimum period:4.431ns(Maximum Frequency:225.683MHz)Minimum Input arrival time before clock:4.818ns Maximum output required time afterclock:2.660ns

Conclusion

Modified Dual-CLCG using CS3A method involves dual coupling off our LCGs that makes it more secure than LCG based PRBGs. However, it is reported that this method has the drawback of generating pseudorandom bit at more delay. Proposed architecture of the new modified dual- CLCG method is significantly reduced the parameter. The proposed architecture of the modified dual-CLCG using three operand PPA method is working with high frequency resultant it would be reduced the delay of the design Based on the performance analysis in terms of hardware complexity, randomness and security, it is observed that 32-bit hardware architecture of the proposed modified dual-CLCG method is optimum and can be useful in the speed of hardware security and IoT applications.

.

References

[1].J.Zhou,Z.Cao,X.Dong,andA.V.Vasilakos,"Security and privacy for cloud-based IoT: Challenges," IEEE Commun. Mag., vol. 55, no. 1, pp. 26–33, Jan. 2017.

[2].Q.Zhang,L.T.Yang,andZ.Chen," Privacy preserving deep computation model on cloud for big data feature learning," IEEE Trans. Comput., vol. 65, no. 5, pp. 1351– 1362, May 2016.

[3].E.Fernandes,A.Rahmati,K.Eykholt,andA.Prakash,"InternetofThingssecurityresearch:Arehashofoldideasornewintellectual challenges?"IEEESecur.Privacy,vol.15,no.4,pp.79–84,2017.

[4].M.Frustaci,P.Pace,G.Aloi,andG.Fortino,"EvaluatingcriticalsecurityissuesoftheIoTworld: Present and future challenges," IEEE Internet Things J., vol. 5, no. 4,pp. 2483–2495, Aug.2018.

[5].E. Zenner, "Cryptanalysis of LFSR-based pseudorandom generators— A survey,"Univ.,MannheimMannheimGermany,2004.

[5].J.Stern,"Secretlinearcongruentialgeneratorsarenotcryptographicallysecure,"inProc.28th Annu. Symp. Found. Comput.Sci.,Oct.1987, pp. 421–426.

[6].D.Xiang,M.Chen,andH.Fujiwara,"Usingweightedscanenablesignalstoimprove test effectiveness of scan-based BIST," IEEE Trans. Comput., vol. 56, no. 12, pp. 1619–1628, Dec. 2007.

[7].L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudo- random number generator," SIAM J. Comput., vol. 15, no. 2, pp. 364–383, 1986.

[8].W. Thomas Cusick, "Properties ofthe x2 mod N pseudorandom number generator,"IEEE Trans. Inf. Theory, vol. 41, no.4, pp.1155–1159, Jul. 1995.

[9].C.Ding,"Blum-Blum-Shubgenerator,"IEEEElectron.Lett.,vol.33,no.8,p.667,Apr.1997.

[10].A.SidorenkoandB.Schoenmakers,"ConcretesecurityoftheBlum-Blum-Shubpseudorandom generator," in Cryptography and Coding (Lecture Notes in Computer Science), vol. 3796. Berlin, Germany: Springer, Nov. 2005, pp. 355–375.

[11].A. K. Panda and C. K. Ray, "FPGA prototype of low latency BBS PRNG," In Proc. IEEE Int. Symp. Nanoelectron. Inf. Syst. (INIS),Indore, India, Dec. 2015, pp.118–123.

[12].P. P. Lopez and E. S. Millan, "Cryptographically secure pseudorandom bit generator forRFID tags,"inProc.Int.Conf.InternetTechnol.SecuredTrans.,London,U.K.,vol.11,Nov.2010, pp. 1–6.

[13].R. S. Katti and R. G. Kavasseri, "Secure pseudo-random bit sequence generation usingcoupled linear congruential generators," in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS),Seattle,WA, USA,May 2008,pp. 2929–2932.

[14].S.Raj Katti andS.Srinivasan,"Efficient hardware implementation of a newpseudo- randombit sequence generator," in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), Taipei, Taiwan, May 2009, pp. 1393– 1396.

[15].R. S. Katti, R. G. Kavasseri, and V. Sai, "Pseudorandom bit generation using coupled congruential maximum- period nonlinear congruential generators derived from the Rényi chaotic map," IEEE Trans.Circuits System.I, Ref. Papers, vol. 54, no. 4, pp. 816–828, Apr. 2007.