ISSN 2277-2685
IJESR/Apr-Jun. 2024/ Vol-14/Issue-2/1053-1062
G Sri Lakshmi *et. al.*, /International Journal of Engineering & Science Research

DESIGN OF MODIFIED DUAL-CLCG ALGORITHM FOR PSEUDO RANDOM BIT GENERATOR

G Sri Lakshmi[1], M Soumya[2], P Varsha[3]

[1]Department of ECE, Bhoj Reddy Engineering College for Women, Hyderabad, India

[2,3,]UG scholar students Department of ECE, Bhoj Reddy Engineering College for Women, Hyderabad, India

ABSTRACT

Pseudorandom bit generator (PRBG) is an essential component for securing data during transmission and storage in various cryptography applications. Among popular existing PRBG methods such as linear feedback shift register (LFSR), linear congruential generator (LCG), coupled LCG (CLCG), and dual-coupled LCG (dual-CLCG), the latter proves to be more secure. This method relies on the inequality comparisons that lead to generating pseudorandom bit at uniform time interval. Hence, a new architecture of the dual- CLCG method is developed that generates pseudo-random bit at uniform clock rate.A new PRBG method called as "modified dual-CLCG" and it's very large-scale integration (VLSI) architecture are proposed in this paper to mitigate the aforesaid problems. The novel contribution of the proposed PRBG method is to generate pseudorandom bit at uniform clock rate with one initial clock delay and minimum hardware complexity.

INTRODUCTION

Security and privacy over the internet is the most sensitive and primary objective to protect data in various Internet-of-Things (IoT) applications. Millions of devices which are connected to the internet generate big data that can lead to user privacy issues. Also, there are significant security challenges to implement the IoT whose objectives are to connect people-to-things and things-to-things over the internet. The pseudorandom bit generator (PRBG) is an essential component to manage user privacy in IoT enabled resource constraint devices. A high bit-rate, cryptographically secure and large key size PRBG is difficult to attain due to hardware limitations which demands efficient VLSI architecture in terms of randomness, area, latency and power. The PRBG is assumed to be random if it satisfies the fifteen benchmark tests of National Institute of Standard anto be random if it satisfies the fifteen benchmark tests of National Institute of Standard and Technology (NIST) standard. Linear feedback shift register (LFSR) and linear congruential generator (LCG) are the most common and low complexity PRBGs. However, these PRBGs badly fail randomness tests and are insecure due to its linearity structure . Numerous studies on PRBG based on LFSR, chaotic map and congruent modulo are reported in the literature. Among these, Blum-Blum-Shub generator (BBS) is one of the proven polynomial time unpredictable and cryptographic secure key generator because of its large prime factorize problem. Although it is secure, the hardware implementation is quite challenging for performing the large prime integer modulus and computing the large special prime integer. There are various architectures of BBS PRBG, discussed in and. Most of them either consume a large amount of hardware area or high clock latency to mitigate it, a low hardware complexity coupled LCG (CLCG) has been proposed . The coupling of two LCGs in the CLCG method makes it more secure than a single LCG and chaotic based PRBGs that generates the pseudorandom bit at every clock cycle . Despite an improvement in the security, the CLCG

method fails the discrete Fourier transform (DFT) test and five other major NIST statistical tests . DFT test finds the periodic patterns in CLCG which shows it as a weak generator. To amend this, Katti et al. proposed another PRBG method, i.e. dual- CLCG that involves two inequality comparisons and four LCGs to generate pseudorandom bit sequence. The dual- CLCG method generates one-bit random output only when it holds inequality equations. Therefore, it is unable to generate pseudorandom bit at every iteration. Hence, designing an efficient architecture is a major challenge to generate random bit in uniform clock time.

To the knowledge of authors, the hardware architecture of the dual-CLCG method is not deeply investigated in the literature and therefore, in the beginning, the architectural mapping of the existing dual-CLCG method is developed to generate the random bit at a uniform clock rate. However, it experiences various drawbacks such as: large usage of flip- flops, high initial clock latency of 2^n for n-bit architecture ,fails to achieve the maximum length period of 2^n (it depends on the number of 0's in the CLCG sequence and is nearly 2^{n-1} for randomly chosen n-bit input seed) and also fails five major NIST statistical tests. Hence, to overcome these shortcomings in the existing dual-CLCG method and its architecture, a new PRBG method and its architecture are proposed in this paper. The manuscript mainly focuses on developing an efficient PRBG algorithm and its hardware architecture in terms of area, latency, power, randomness and maximum length sequence.

Literature survey

P. L. Montgomery, "Modular multiplication without trial division," Math. Comput.We present a method for multiplying two integers (called *N-residues*) modulo *N* while avoiding division by *N*. *N*-residues are represented in a nonstandard way, so this method is useful only if several computations are done modulo one *N*. The addition and subtraction algorithms are unchanged.

S.-R. Kuang, K.-Y. Wu, and R.-Y. Lu, "Low-cost high-performance VLSI architecture for montgomery modular multiplication," The paper proposes a Montgomery Modular Multiplier (MMM) using a simple and efficient Montgomery multiplication algorithm. Here a modification in the form of using hybrid full adders in the Carry Save adder is proposed. The hybrid full adder is designed using a conventional Complementary Metal Oxide Semiconductor and transmission gate logic. There is about 54% and 55% reduction of area (no. of components) in Radix 2 MMM and Semi-Carry-Save (SCS) based MMM with hybrid full adders. There is significant reduction in the power dissipation of 52% for Radix 2 MMM and 46% of SCS based MMM when hybrid adders are used instead of C-CMOS Full-Adders. The delay is also reduced by 47% in SCS based MMM as compared to that of Radix 2 MMM. The software used are Xilinx ISE 14.2 and Mentor Graphics Pyxis Schematic in 180-nm technology.

S.-R. Kuang, J.-P. Wang, K.-C. Chang, and H.-W. Hsu, "Energy-efficient high-throughput montgomery modular multipliers for RSA cryptosystems,"For future internet services and data communication systems, it is identified that security matters become questionable and problematical. Cryptographic algorithms are a convenient tool for achieving security in those systems. So, realization of cryptographic systems in hardware is more advantageous. Of the two-broad category of cryptographic systems as public key cryptosystems and secret key cryptosystems, public key cryptosystems are widely used. In many public key

cryptosystems, the key operation is modular multiplication with large input operands. The trial division in modular multiplication is time consuming. So, well-known algorithm called Montgomery modular multiplication algorithm is introduced by avoiding the trial division. Shifting modular additions are used instead of complicated division operations. Different modifications to conventional Montgomery modular multiplications are proposed to reduce the delay associated with the long carry propagation in the computation of intermediate result. This paper explores a comparison between two modification algorithms to conventional Montgomery MM algorithms

S. S. Erdem, T. Yanik, and A. Celebi, "A general digit-serial architecture for montgomery modular multiplication," Multiplication is a key operation to perform the processing speed of digital processor. Montgomery multiplication is a strategy for performing quick modular multiplication. This paper presents an outline on execution of Montgomery measured duplication estimation utilizing VLSI design. The Montgomery figuring is a fast particular increase procedure as regularly as conceivable used in cryptographic applications, in which the capability of cryptosystem depends upon the speed of secluded duplication. This audit gives the assessment between different adjustments done in Montgomery particular augmentation.

R. S. Katti and S. K. Srinivasan, "Efficient hardware implementation of a new pseudo-random bit sequence generator''In this work, the architecture of a dual-coupled linear congruential generator (dual-CLCG) for pseudo-random bit generation is proposed to improve the speed of the generator and minimize power dissipation with the optimum chip area. To improve its performance, a new pseudo-random bit generator (PRBG) employing two-operand modulo adder and without shifting operation-based dual-CLCG architecture is proposed. The novelty of the proposed dual-CLCG architecture is the designing of LCG based on two-operand modulo adder rather than a three-operand one and without using shifting operation as compared to the existing LCG architecture. The aim of the work is to generate pseudo-random bits at a uniform clock rate at the maximum clock frequency and achieve maximum length of the random bit sequence. The power dissipation with the optimum chip area of PRBG is also observed for the proposed architecture. The generated sequence passes all the 15 tests of the National Institute of Standards and Technology (NIST) standard. Verilog HDL code is used for the design of the proposed architecture. Its simulation is done on commercially available Spartan-3E FPGA (ISE Design Suite by Xilinx) as well as on 90-nm CMOS technology (Cadence tool).

MODIFIED DUAL CLCG USING BINARY ADDER TECHNIQUE

The three-operand binary addition is one of the critical arithmetic operation in the congruential modular arithmetic architectures and LCG-based PRBG methods such as CLCG , MDCLCG and CVLCG . It can be implemented either by using two stages of two-operand adders or one stage of three-operand adder. Carry-save adder (CSA) is the commonly used technique to perform the three-operand binary addition. It computes the addition of three operands in two stages. The first stage is the array of full adders. Each full adder computes "carry" bit and "sum" bit concurrently from three binary input ai, bi and ci . The second stage is the ripple-carry adder that computes the final n-bit size "sum" and one-bit size "carry-out" signals at the output of three-operand addition. The "carry-out" signal is propagated through the n number of full adders in the ripple-carry stage. Therefore, the delay increases linearly with the increase of bit length. The architecture of the three-operand carry-save adder is shown in Fig. 1 and the critical path delay is highlighted with a dashed line. It shows that the critical path delay depends on the carry propagation delay of ripple carry stage and is evaluated as follows

$T_{CS3A} = (n+1)T_{FA} = 3T_X + 2nT_G$

Similarly, the total area is evaluated as follows,

$A_{CS3A} = 2nA_{FA} = 4nA_X + 6nA_G$

Here, A_G and T_G indicate the area and propagation delay of basic 2-input gate (AND/OR/NAND/NOR) respectively. A_X and T_X indicate the area and propagation delay of 2-input XOR gate respectively. The major drawback of the CS3A is the larger critical path delay which increases with an increase of bit length. This critical propagation path delay influences the overall latency of the congruential modular arithmetic based cryptography and PRBG architectures, where three-operand adder is the primary component.

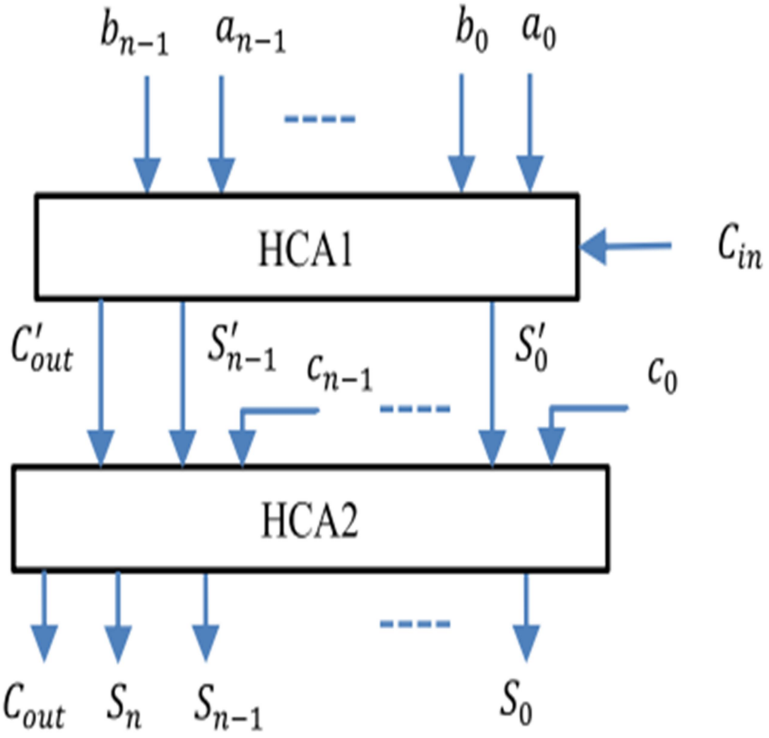

Fig. 1. Block level architecture of HCA-based three-operand adder (HC3A).

Hence, to shorten the critical path delay, two stages of parallel prefix two-operand adder can also be used. In literature, parallel prefix or logarithmic prefix adders are the fastest twooperand adder techniques . These adder techniques have six different topologies, such as Brent-Kung, Sklansky, Knowles, Ladner-Fischer, Kogge-Stone (KS) and Han-Carlson (HC). Among these, Han-Carlson is the fastest one when bit size increases (i.e. n > 16) . In recent years, various such kind of parallel prefix two-operand adders, i.e., Ling Jackson-Talwar , ultra-fast adder , hybrid PPFCSL and hybrid Han-Carlson are also discussed in the literature. The ultra-fast adder is reported as the fastest one, and it is even faster than the Han-Carlson by three gates delay. However, it consumes comparatively two times large gate area than the Han-Carlson adder. On the other hand, the hybrid Han-Carlson adder is designed with two Brent-Kung stages each at the beginning and the end, and with Kogge-Stone stages in the middle. This resultant a slightly higher delay (two gates delay) than the Han Carlson adder, with a 10% to 18% reduction in the gate complexity.

Essentially, the Han-Carlson adder provides a reasonably good speed at low gate complexity as compared to other existing two-operand adder techniques. It has the lowest areadelay product (ADP) and power-delay

product (PDP) among all. Thus, the three-operand addition can be performed using Han-Carlson adder (HCA) in two stages, as shown in Fig. 2. The detailed architecture of HCA-based three-operand adder (HC3A) is presented in . The maximum combinational path delay of HC3A depends on the propagate chain, i.e. the number of black-grey cell stage in the PG logic of Han-Carlson adder and is evaluated as follows,

$$T_{HC3A} \approx 4T_X + 4\lfloor \log_2 n \rfloor T_G$$

$$A_{HC3A} \approx (4n+1)A_X + 6\left[n + \left\lceil \frac{n}{2} \right\rceil s - 2^s + 1\right] A_G$$

Here,

$$s = \lceil \log_2 n - 1 \rceil$$

The HCA-based three-operand binary adder (HC3A) greatly reduces the critical path delay in comparison with the three-operand carry-save binary adder. However, the area increases with increase of bit length in the order of O(n log2 n). Therefore, to minimize this trade-off between area and delay, a new high-speed, area-efficient three-operand adder technique and its efficient VLSI architecture is proposed in the next section

A Three operand binary adder is the basic functional unit to perform the pseudorandom bit generator algorithms and in various cryptography. The basic method used to perform the three-operand binary addition is carry save adder, which leads to high delay. For this a parallel prefix two operand adder such as Han-Carlson adder is used to reduce the delay but increases the hardware architecture i.e., area increases. To overcome this disadvantage, we need a new area efficient and high-speed adder architecture to be proposed using pre compute bitwise addition followed by carry prefix computation logic to perform three operand binary adder which reduces delay and area efficiently. This method is the proposed method and implemented on the FPGA device. A newly designed three operand binary adder is shown and is implemented in MDCLCG. The results of 16 bit and 32-bit three operand adder will be shown and this proposed method is applied on Modified Dual CLCG. The Carry-Save-Adder architecture used in 32-bit MDCLCG is replaced by the proposed architecture. The design is prototyped on a commercially available FPGA platform to validate the design on silicon chip.

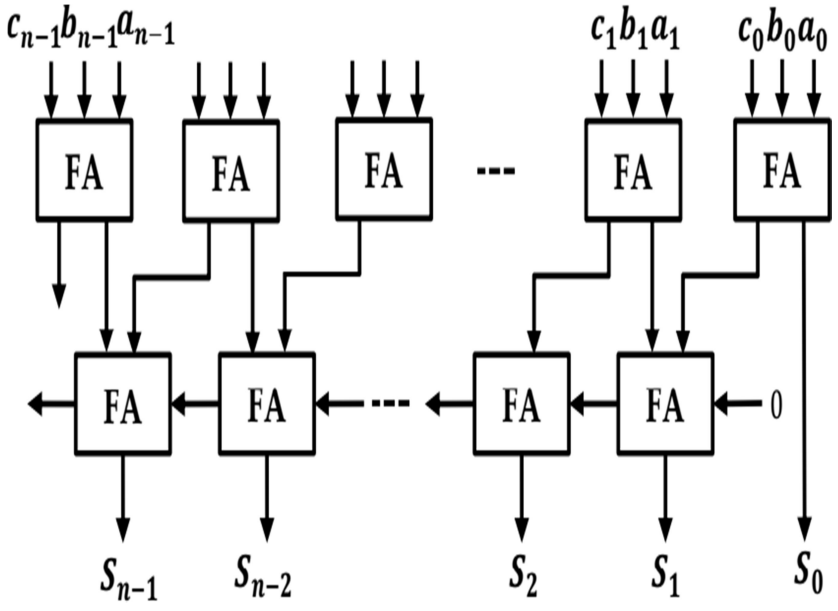

Fig. 2. Three-operand carry-save adder (CS3A).

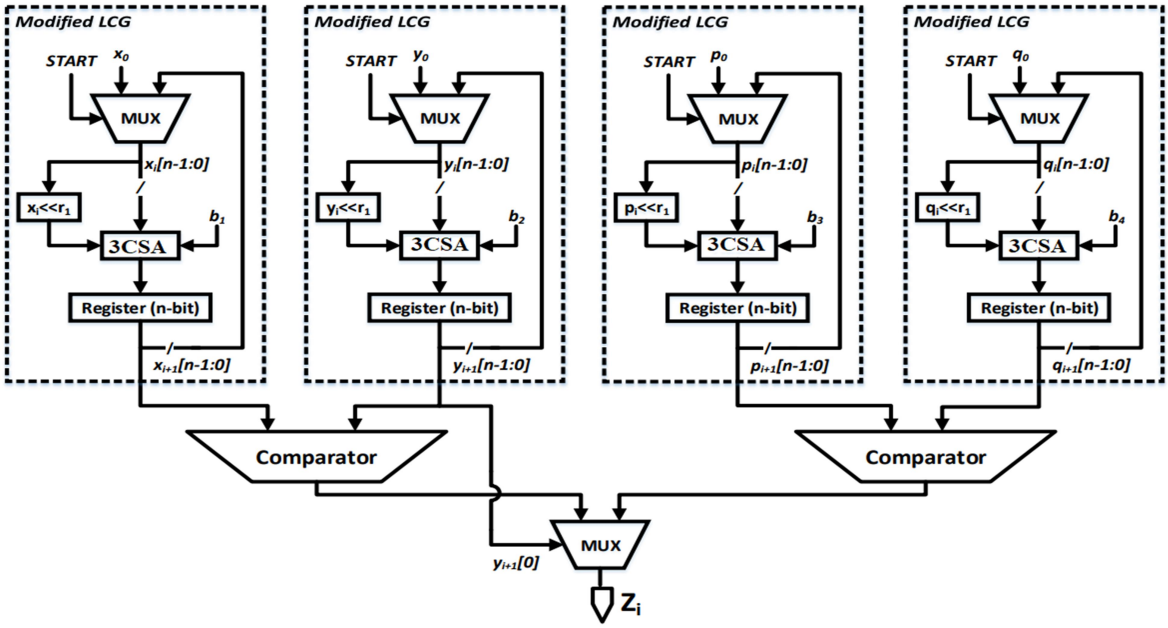

Fig .3. MDCLCG

RESULTS

RTL SCHEMATIC:- 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 represented below shows the RTL schematic diagram of the designed architecture.

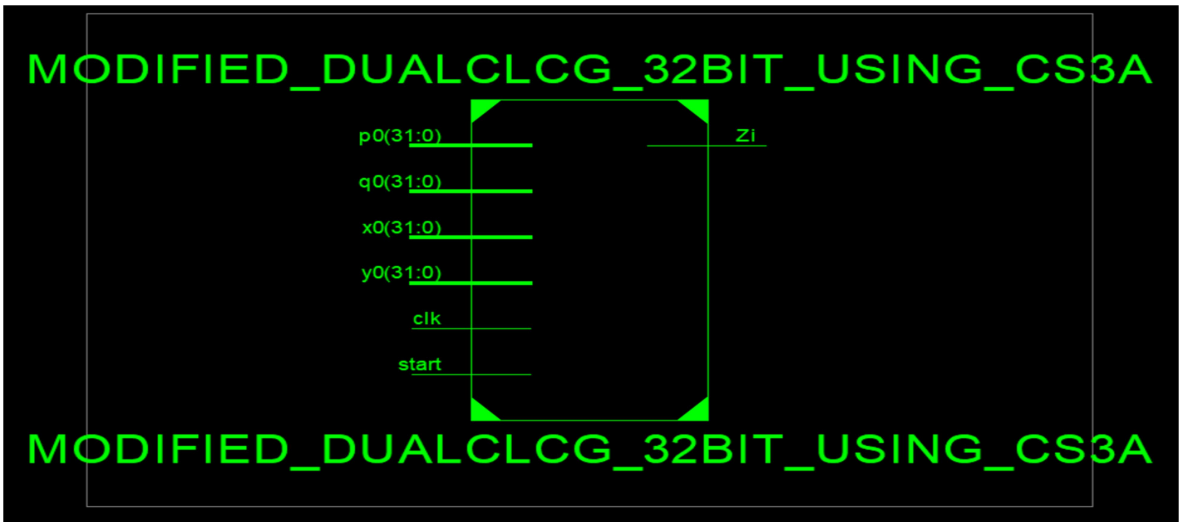

Fig 4: RTL Schematic view of Modified Dual CLCG using CS3A

TECHNOLOGY SCHEMATIC:- The technology schematic makes the representation of the architecture in the

LUT format ,where the LUT is consider as the parameter of area 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.

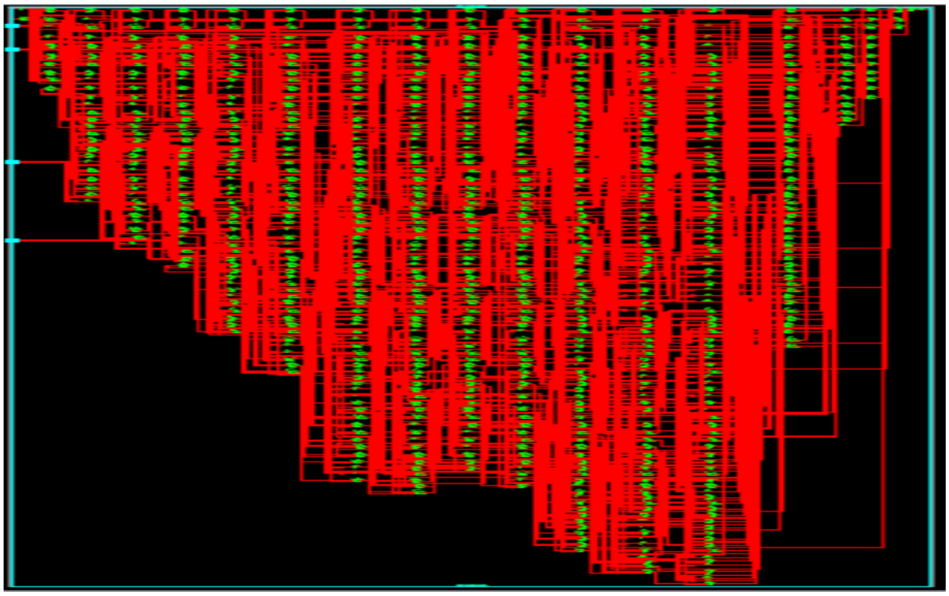

Fig 5: View technology Schematic of modified Dual CLCG using CS3A

Simulation

The simulation is the process which is termed as the final verification in respect to its working where as 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 out put. Here it has the flexibility of providing the different radix number systems.

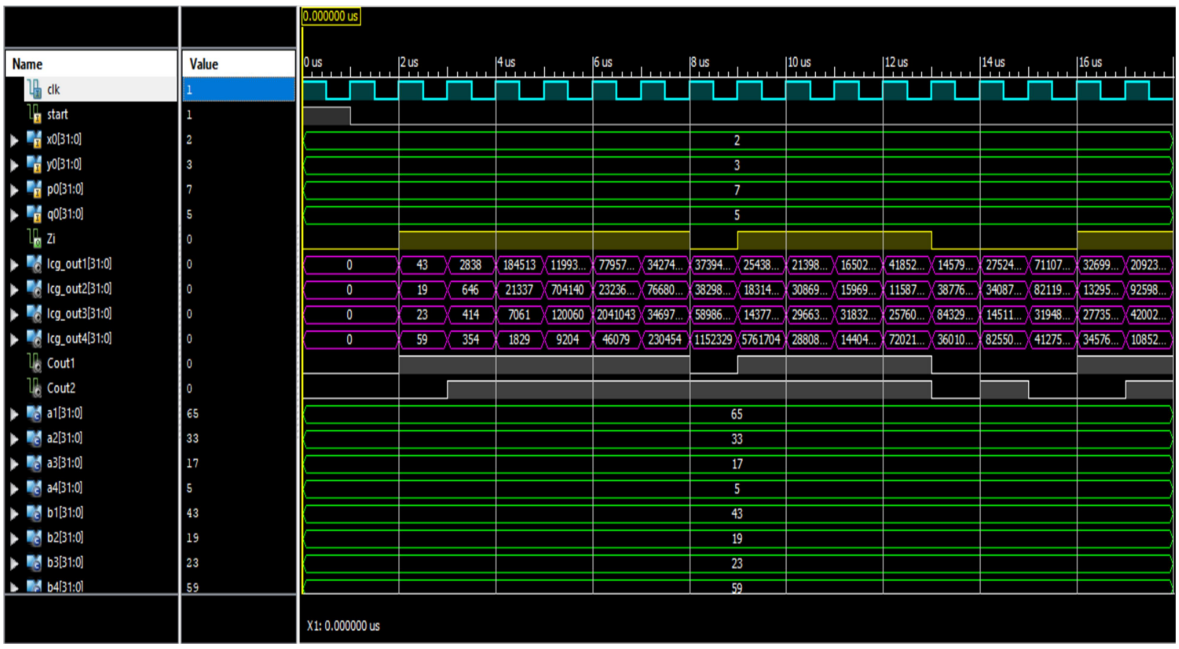

Fig 6: simulated wave form of modified Dual CLCG using CS3A

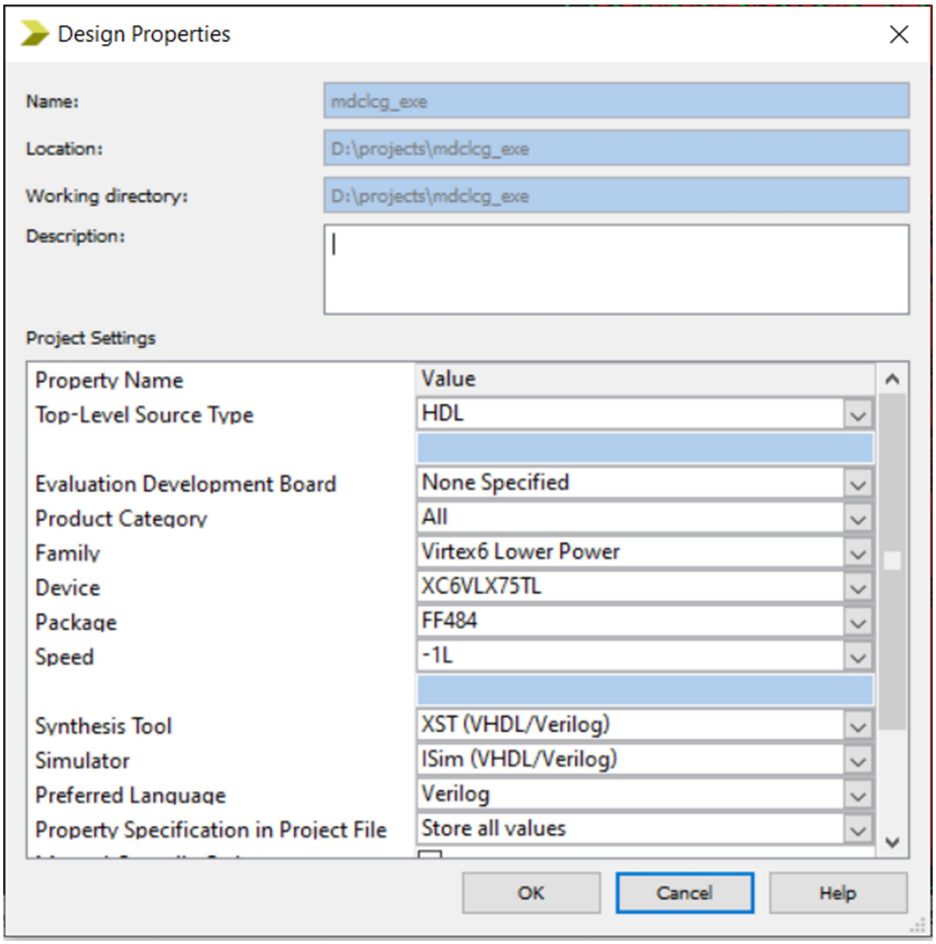

Fig 7 : family selected for synthesis

PARAMETERS:-

Consider in VLSI the parameters treated are area ,delay ,frequency and power ,based on these parameters one can judge the one architecture to other. here the consideration of area and power consumptions are considered the parameters are obtained by using the tool XILINX 14.7 and the HDL is verilog language .when frequency is more for any design it will increase the speed of design.

Parameter	For modified dual CLCG design
Frequency (MHz)	132.714

Table : parameter comparison

CONCLUSION

Modified Dual-CLCG using CS3A method involves dual coupling of four LCGs that makes it more secure than LCG based PRBGs. The proposed architecture of the new modified dual- CLCG method is significantly 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, and A. 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, and Z. Chen, "Privacy preserving deep computa- tion 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, and A. Prakash, "Internet of Things security research: A rehash of old ideas or new intellectual challenges?" IEEE Secur. Privacy, vol. 15, no. 4, pp. 79–84, 2017.

[4] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: 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. Mannheim, Mannheim, Germany, 2004. [Online]. Available: http://orbit.dtu.dk/en/publications/cryptanalysis-of-lfsrbased- pseudorandom-generators–a-survey(59f7106b-1800-49df-8037- fbe9e0e98ced).html

[6] J. Stern, "Secret linear congruential generators are not cryptographically secure," in Proc. 28th Annu. Symp. Found. Comput. Sci., Oct. 1987, pp. 421–426.

[7] D. Xiang, M. Chen, and H. Fujiwara, "Using weighted scan enable signals to improve test effectiveness of scan-based BIST," IEEE Trans. Comput., vol. 56, no. 12, pp. 1619–1628, Dec. 2007.

[8] 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.

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

[10] C. Ding, "Blum-Blum-Shub generator," IEEE Electron. Lett., vol. 33, no. 8, p. 667, Apr. 1997.

[11] A. Sidorenko and B. Schoenmakers, "Concrete security of the Blum- Blum-Shub pseudorandom generator," in Cryptography and Coding (Lecture Notes in Computer Science), vol. 3796. Berlin, Germany: Springer, Nov. 2005, pp. 355–375.

[12] 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.

[13] P. P. Lopez and E. S. Millan, "Cryptographically secure pseudorandom bit generator for RFID tags," in Proc. Int. Conf. Internet Technol. Secured Trans., London, U.K., vol. 11, Nov. 2010, pp. 1–6.

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

[15] S. Raj Katti and S. Srinivasan, "Efficient hardware implementation of a new pseudo-random bit sequence

generator," in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), Taipei, Taiwan, May 2009, pp. 1393–1396.

[16] R. S. Katti, R. G. Kavasseri, and V. Sai, "Pseudorandom bit generation using coupled congruential generators," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 57, no. 3, pp. 203–207, Mar. 2010.

[17] Revised NIST Special Publication 800-22. (Apr. 2010). A Statistica Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications. [Online].
Available: http://csrc.nist.gov/publications/nistpubs/800-22-rev1.pdf

[18] Random Integer Generator. Accessed: Feb. 20, 2018. [Online]. Avail- able: https://www.random.org/integers

[19] T. Addabbo, M. Alioto, A. Fort, A. Pasini, S. Rocchi, and V. Vignoli, "A class of 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.

[20] J. Massey, "Shift-register synthesis and BCH decoding," IEEE Trans. Inf. Theory, vol. IT-15, no. 1, pp. 122–127, Jan. 1969.

[21] R. Ostrovsky, Foundations of Cryptography (Lecture Notes). Los Ange- les, CA, USA: UCLA, 2010.

[22] O. Goldreich, Foundations of Cryptography. New York, NY, USA: Cambridge Univ. Press, 2004.

[23] J. Katz and Y. Lindell, Introduction to Modern Cryptography. Boca Raton, FL, USA: CRC Press, 2008.

[24] M. Luby, Pseudo Randomness and Cryptographic Applications. Princeton, NJ, USA: Princeton Univ. Press, 1996.

[25] T. Kim, W. Jao, and S. Tjiang, "Circuit optimization using carry-save- adder cells," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 17, no. 10, pp. 974–984, Oct. 1998.

[26] S.-W. Cheng, "A high-speed magnitude comparator with small transistor count," in Proc. ICECS, vol. 3, 2003, pp. 1168–1171.