International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

HIGH-ACCURACY AREA-EFFICIENCY VLSI ARCHITECYURE OF THREE-OPERAND BINARY ADDER

DAVULURI MOUNIKA, Dr.T.RAGHAVENDRA VISHNU, M.Tech, Ph.D.
Department of Electronics and Communication Engineering Priyadarshini Institute of Technology & Science for Women
Professor & HOD Department of Electronics and Communication Engineering Priyadarshini Institute of Technology & Science for Women

ABSTRACT: Three-operand binary adder is the basic functional unit to perform the modular arithmetic in various cryptography and pseudorandom bit generator (PRBG) algorithms. Square root carry select adder used for three-operand addition that significantly reduces the critical path delay at the cost of additional hardware. Hence, a new high-speed and area-efficient adder architecture is proposed RCA logics to perform the three-operand binary addition that consumes substantially less area, low power and drastically reduces the adder delay. The proposed architecture is implemented on the FPGA device for functional validation and also synthesized with the commercially available 32nm CMOS technology library. Moreover, it has a lesser area and lower power dissipation Also, the proposed adder achieves less area than the existing three-operand adder techniques.

Index Terms— Three- operand adder, square root carry select adder, modular arithmetic.

1. INTRODUCTION

In many Internet-of-Things (IoT) applications, data security and privacy are of utmost importance. The proliferation of internet-connected devices generates vast volumes of data that may jeopardise the privacy of those using them. Security is a major challenge when adopting the Internet of Objects, It seeks to connect people and objects over the internet PRBGs (pseudorandom bit generators) are critical in ensuring user privacy in IoT devices with limited resources. The National Institute of Standards and Technology (NIST) has set fifteen benchmark tests for the PRBG, and if it passes them, it is deemed random. These two types of PRBG are the most often used and least complicated: linguistic feedback shift registers and linear congruential generators (LCG). These PRBGs, on the other hand, fail randomization tests because of their linearity structure and are hence unsafe. Several studies have been done on PRBG using LFSR, In the literature, there are references to chaotic maps and congruent modulo.BBS is one of the confirmed polynomial-time unpredictable and cryptographic secure key generators due to its enormous prime factorization difficulty. Hardware implementation of the big prime integer modulus and computation of the large special prime integer is challenging, even if it is secure. BBS PRBG designs are available in a variety of styles.It was intended to address the issue that most of them either need a lot of hardware space or have a lot of clock delay.In contrast to chaotic PRBGs and single LCGs, the CLCG technique employs two LCGs to generate the pseudorandom bit for each clock cycle, which makes it more safe.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

This technique, although a higher level of security, The discrete Fourier transform (DFT) test, as well as five other main NIST statistical tests, fail. CLCG exhibits periodic patterns in DFT studies, showing that it is a weak source. Katti et al. developed a PRBG approach that exploits pseudorandom bit sequences by combining two inequality comparisons and four LCGs. When holding inequality equations, the dual-CLCG approach only provides one-bit random output. It is difficult to generate pseudorandom bits every time. Therefore, designing an efficient architecture that can output random bits in a constant clock time is an enormous challenge.

Because there is no research on how to design a random bit generator using the dual-CLCG methodology, authors of this paper constructed a hardware architecture mapping first to generate the random bit at a constant clock rate. Clock latency of 2n and inability to meet maximum period length make CLCG algorithm unsuitable for n-bit systems, where the number of 0s in the CLCG sequence determines the period length, which is nearly 2n1 for a randomly chosen n-bit input seed. CLCG algorithm fails to pass five major NIST statistical tests.These findings lead the authors to propose a new PRBG methodology and design to solve the shortcomings of their Previously, a dual-CLCG approach and architecture were used. Providing an efficient PRBG algorithm and supporting hardware design in terms of space, delay, power, randomness and maximum sequence length is the major objective of the project.

Consider the following to give you an overview of how the document is structured: Using an architectural mapping of the dual-CLCG approach, the suggested PRBG methodology and randomization features are given. The VLSI design of the improved dual-CLCG technique.As the name indicates, a Combined Linear Congruential Generator (CLCG) is a sort of PRNG (pseudorandom number generator) that combines two or more LCGs (linear congruential generators). Combining two or more LCGs into a single random number generator can result in a significant increase in the generator's period length, making it more suited for modelling more complicated systems. The following is the definition of the combination linear congruential generator algorithm:

$$\mathrm{Xi} \equiv \left(\sum_{j=1}^{k} (-1\dot{)}^{j-1} \mathrm{Y_{ij}}\right)(\mathrm{mod}(\mathrm{m1}-1))$$

Where m1m1 is the LCG's modulus, Yi,j is the jth LCG's ith input, and XiXi is the ith randomly generated value. In Efficient and Portable Combination Random Number Generators for 32-bit Processors, L'Ecuyer discusses a combined linear generator that employs two LCGs.

Using Katti et aldual-CLCG .'s approach, four linear congruential generators are coupled in a mathematically defined dual coupling.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

$$x_{i+1} = a_1 \times x_i + b_1 \bmod 2^n \quad (1)$$

$$y_{i+1} = a_2 \times y_i + b_2 \bmod 2^n \quad (2)$$

$$p_{i+1} = a3 \times p_i + b3 \bmod 2^n \quad (3)$$

$$q_{i+1} = a4 \times q_i + b4 \bmod 2^n \quad (4)$$

$$Z_i = \begin{cases} 1 & \text{if } x_{i+1} > y_{i+1} \text{ and } p_{i+1} > q_{i+1} \\ 0 & \text{if } x_{i+1} < y_{i+1} \text{ and } p_{i+1} < q_{i+1} \end{cases} \quad (5)$$

An alternate method for calculating Zi's output sequence is presented in], i.e..,

$$Zi = Bi \text{ if } Ci = 0 \quad (6)$$

Where,

$$B_i = \begin{cases} 1, & \text{if } x_{i+1} > y_{i+1} \\ 0, & \text{else} \end{cases}; \quad C_i = \begin{cases} 1, & \text{if } p_{i+1} > q_{i+1} \\ 0, & \text{else} \end{cases} \quad (7)$$

At the top of this page, you'll find the constant parameters, as well as the starting seed values, for each of these variables: A1, B1, A2, B2, A3, B3, A4, B4, and so on. For maximum time, the following requirements must be met.

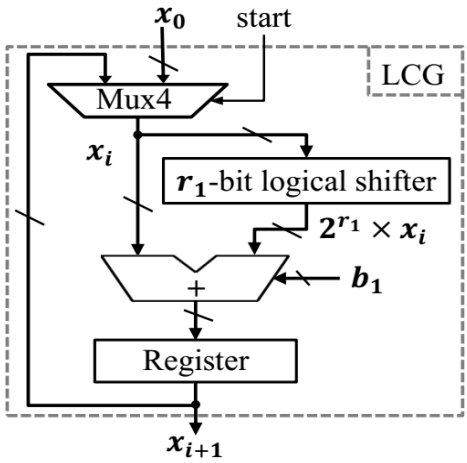

Fig. 1. Architecture of the linear congruential generator.

(i) With 2n, b1, b2, b3, and b4 are comparatively prime (m).

(ii) The numbers a1-1, a2-1, a3-1, and a4-1 must be divisible by four.

As long as Ci is "zero" in the dual-CLCG approach, Bi is selected as output; otherwise, no binary value is provided. As a result, it is impossible to generate pseudorandom bits using the dual-CLCG technique.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

2. LITERATURE SURVEY

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.

THREE-OPERAND ADDER ARCHITECTURE

This section presents a new adder technique and its VLSI architecture to perform the three-operand addition in modular arithmetic. The existed adder technique is a parallel prefix adder. However, it has four-stage structures instead three-stage structures in prefix adder to compute the

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

addition of three binary input operands such as bit-addition logic, base logic, PG (propagate and generate) logic and sum logic. The logical expression of all these four stages are defined as follows,

Stage-1: Bit Addition Logic:

$$S'_i = a_i \oplus b_i \oplus c_i,$$
$$cy_i = a_i \cdot b_i + b_i \cdot c_i + c_i \cdot a_i$$

Stage-2: Base Logic

$$G_{i:i} = G_i = S'_i \cdot cy_{i-1}, \quad G_{0:0} = G_0 = S'_0 \cdot C_{in}$$
$$P_{i:i} = P_i = S'_i \oplus cy_{i-1}, \quad P_{0:0} = P_0 = S'_0 \oplus C_{in}$$

Stage-3: PG (Generate and Propagate) Logic

$$G_{i:j} = G_{i:k} + P_{i:k} \cdot G_{k-1:j},$$
$$P_{i:j} = P_{i:k} \cdot P_{k-1:j}$$

Stage-4: Sum Logic:

$$S_i = (P_i \oplus G_{i-1:0}), \quad S_0 = P_0, \; C_{out} = G_{n:0}$$

The existed VLSI architecture of the three-operand binary adder and its internal structure is shown in Fig. 3. The new adder technique performs the addition of three n-bit binary inputs in four different stages. In the first stage (bit-addition logic), the bitwise addition of three n-bit binary input operandsis performed with the array of full adders, and each full adder computes "sum (S'_i)" and "carry (cyi)" signals as highlighted in Fig. 3(a). The logical expressions for computing sum (S'_i) and carry (cyi) signals are defined in Stage-1, and the logical diagram of the bit-addition logic is shown in Fig. 3(b). In the first stage, the output signal "sum (S'_i)" bit of current full adder and the output signal "carry" bit of its right-adjacent full adder are used together to compute the generate (Gi) and propagate (Pi) signals in the second stage (base logic). The computation of Gi and Pi signals are represented by the "squared saltire-cell" as shown in Fig. 3(a) and there are n+1 number of saltire-cells in the base logic stage. The logic diagram of the saltire-cell is shown in Fig. 3(b), and it is realized by the following logical expression,

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

$$G_{i:i} = G_i = S'_i \cdot cy_{i-1};$$
$$P_{i:i} = P_i = S'_i \oplus cy_{i-1}$$

The external carry-input signal (Cin) is also taken into consideration for three-operand addition in the proposed adder technique. This additional carry-input signal (Cin) is taken as input to base logic while computing the G0 ($S'_0 \cdot$ Cin) in the first saltire-cell of the base logic. The third stage is the carry computation stage called "generate and propagate logic" (PG) to pre-compute the carry bit and is the combination of black and grey cell logics. The logical diagram of black and grey cell is shown in Fig. 3(b) that computes the carry generate Gi: j and propagate Pi: j signals with the following logical expression,

$$G_{i:j} = G_{i:k} + P_{i:k} \cdot G_{k-1:j},$$
$$P_{i:j} = P_{i:k} \cdot P_{k-1:j}$$

The number of prefix computation stages for the proposed adder is (log2 n+1), and therefore, the critical path delay of the proposed adder is mainly influenced by this carry propagate chain. The final stage is represented as sum logic in which the "sum (Si)" bits are computed from the carry generate Gi: j and carry propagate Pi bits using the logical expression, Si = (Pi ⊕ Gi−1:0). The carryout signal (Cout) is directly obtained from the carry generate bit Gn:0.

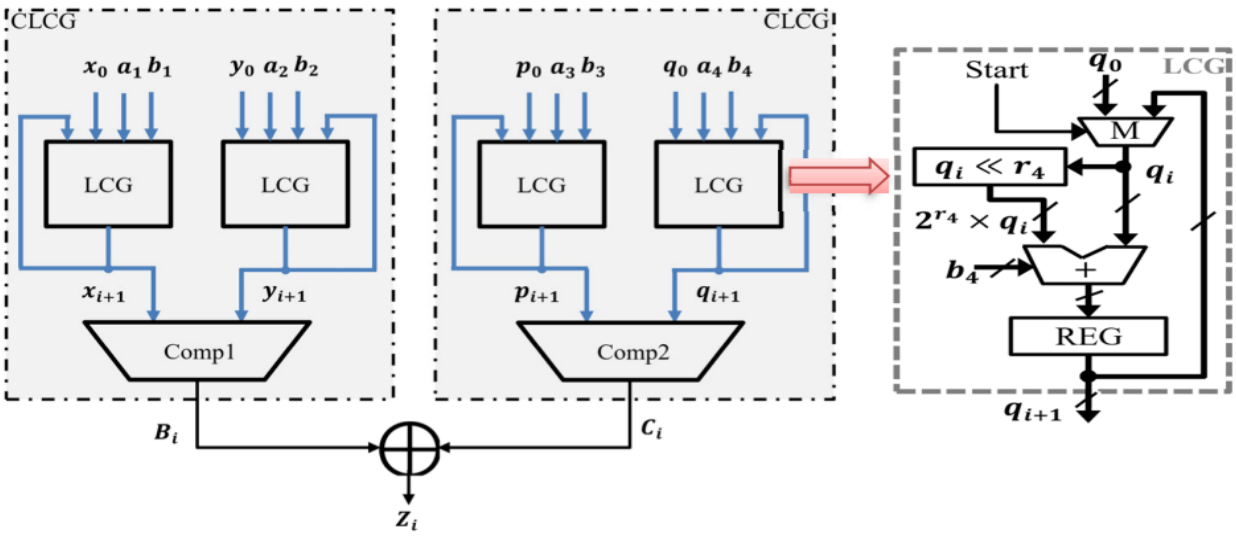

Fig. 4. MDCLCG architecture

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

The performance of the proposed adder is further mesured by incorporating the design in the modified dual-CLCG (MDCLCG) PRBG method for high data rate lightweight hardware security in the field of IoT applications.

PERFORMANCE OF THE MODIFIED DUAL-CLCG ARCHITECTURE WITH THE THREE-OPERAND ADDER

The hardware security in the field of IoT applications demands stream-cipher based high data rate, lightweight cryptography technique for fastest encryption/ decryption. Key generator or pseudorandom bit generator (PRBG) is the primary component in the stream-cipher based encryption/ decryption. Modified dual-CLCG (MDCLCG) is the most efficient PRBG method amongst the existing PRBG methods which is suitable for stream-cipher based hardware security. However, the security strength of the MDCLCG method linearly depends on the bit size of the congruential modulus. It is polynomial-time unpredictable and secure if $n \geq 32$- bits [10]. The hardware architecture of the MDLCG method is based on LCG, as shown in Fig. 4 in which three-operand modulo2n adder is the primary computational arithmetic block. The MDCLCG architecture presented in [10] is developed with four three-operand modulo-2n carry-save adders (CS3A) and two magnitude comparators along with four registers andmultiplexers. The longer carry propagation gate delay in CS3A adder influences the performance of MDCLCG architecture with an increase of bit size. Therefore, in this section, the performance metrics of the MDCLCG are measured by replacing the CS3A adder with the HHC3A and proposed adder architectures. By considering the operation of three-operand modulo-2n addition in MDCLCG method, the architecture of the proposed adder is further redesigned.

Square Root Carry SelectAdder

Carry Select Adder consists of two rca blocks.in this project to reduce the optimal delay we proposed square root carry selectadder.In Square Root Carry Select Adder (SRCSA), [9]-[10] the block size can be variable. The complete analysis is omitted here for brevity, but here, e.g., a 16-bit adder can be created using block sizes of 2-2-3-4-5 instead of using uniform block size of four (as done before) [8]. This break-up is ideal when the Full-Adder delay is equal to the MUX

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

delay. Fig. 6 shows the block diagram of proposed SRCSA adder for 16 bits where the inputs are A and B, Carry-in is denoted as Cin and outputs are denoted by sum (S) and Carry-out(Cout).

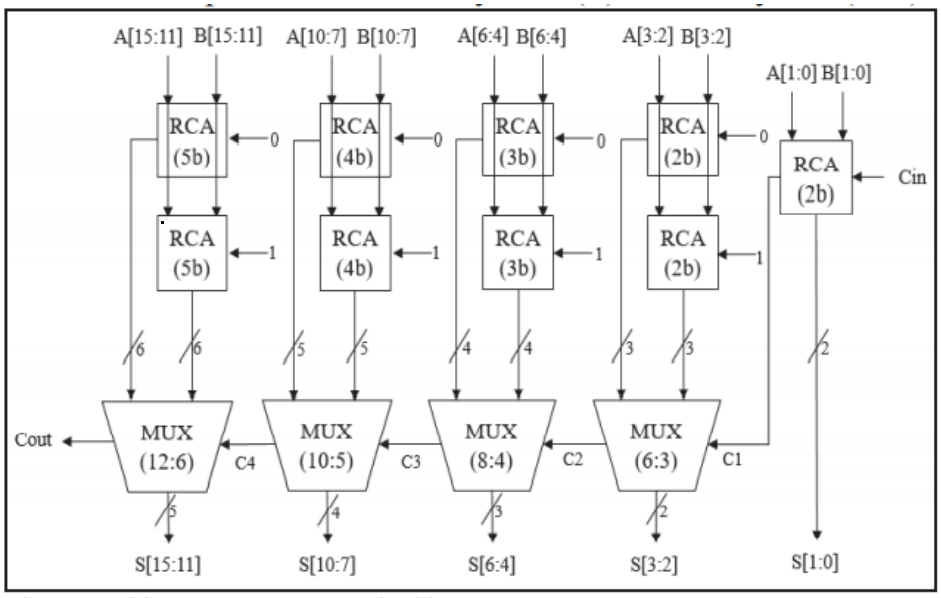

Fig. 6. 16-bit SRCSA (proposed adder)

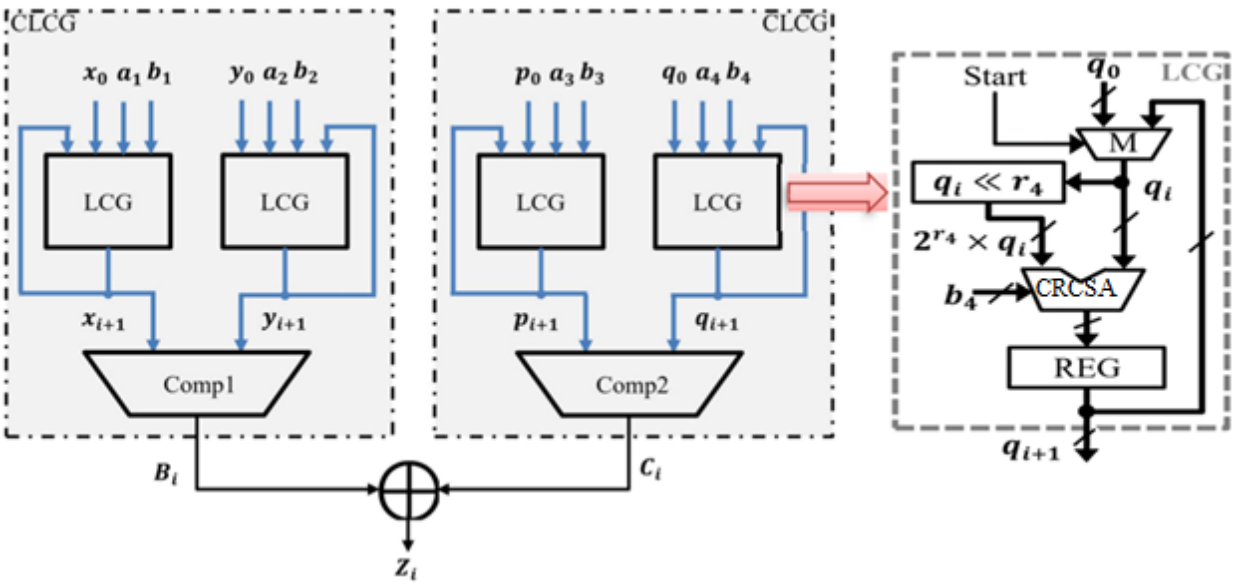

Fig. 7. MDCLCG architecture Using CRCSA

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

4.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.everilog ,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.

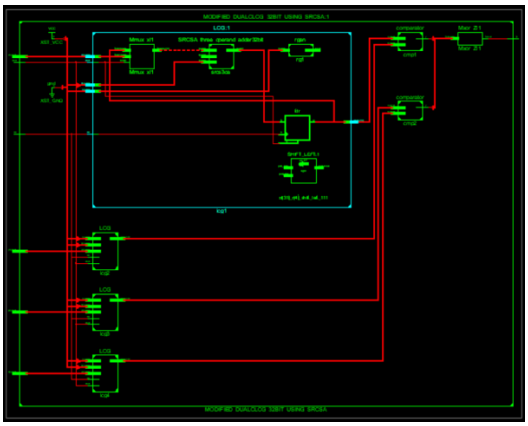

Fig3: RTL Schematic of Proposed MDCLCG

TECHNOLOGY SCHEMATIC:-The architecture is represented in the LUT format by the technology schematic, where the LUT is a parameter of area that is utilised in VLSI to estimate the architecture design. The LUT is a square unit that represents the memory allocation of the code in FPGA.

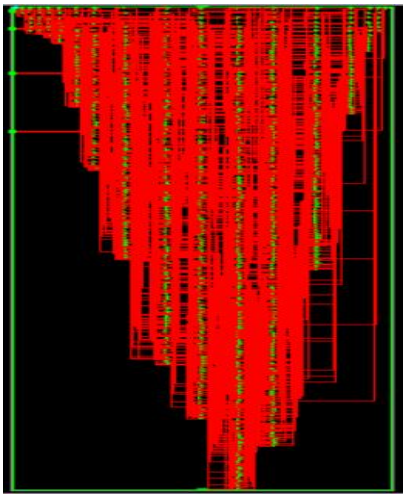

Fig4:View Technology Schematic of proposed MDCLCG

SIMULATION:-The system's operation is verified by simulation, whilst the connections and blocks are verified through the schematic technique. The simulation window, which can only

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

display waveforms, is opened by selecting 'implantation to simulation' from the tool's main screen. In this scenario, it may provide a variety of radix number systems.

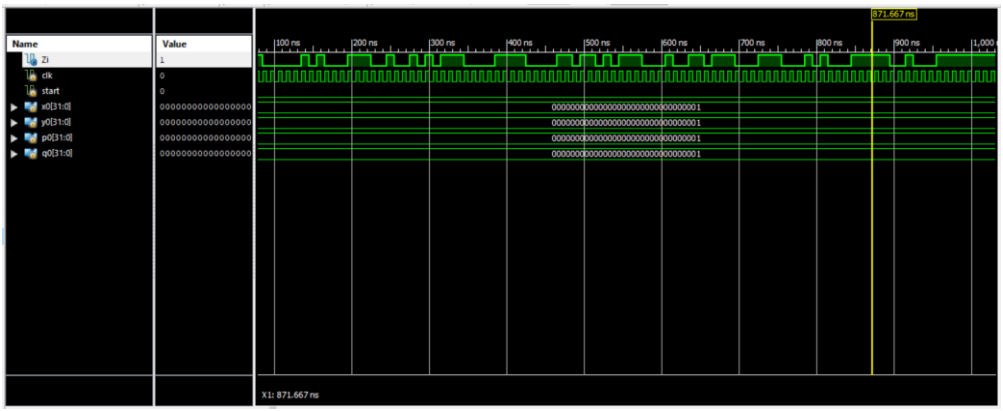

Fig5:Simulated Waveforms of proposed MDCLCG

PARAMETERS:-Consider the parameters of area, delay, and power in VLSI; these factors may be used to compare one architecture to another. The parameter is calculated using the tool XILINX 14.7, and the HDL language used is verilog.

Parameter	Existed MDCLCG	Proposed MDCLCG
No of LUTs	715	646

Table 1: parameter comparison

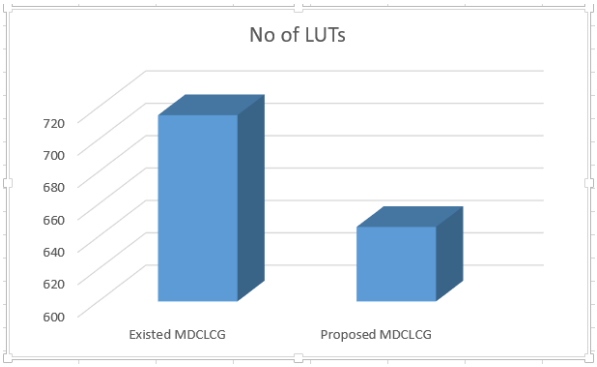

Fig6: LUT comparison bargraph

Conclusion

Modified Dual-CLCG method involves dual coupling of four 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 large area and more delay. proposed architecture of the new modified dual- CLCG method using square root carry select adder is significantly reduced the area of the design. The proposed architecture of the modified dual- CLCG method is

prototyped on the commercially available FPGA devices and the results are captured in real-time using Xilinx chip scope for validation. 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 less area of hardware security and IoT applications ,cryptography and PRBG applications.

REFERENCES

[1] M. M. Islam, M. S. Hossain, M. K. Hasan, M. Shahjalal, and Y. M. Jang, "FPGA implementation of high-speed area-efficient processor for elliptic curve point multiplication over prime field," IEEE Access, vol. 7, pp. 178811–178826, 2019.

[2] Z. Liu, J. GroBschadl, Z. Hu, K. Jarvinen, H. Wang, and I. Verbauwhede, "Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the Internet of Things," IEEE Trans. Comput., vol. 66, no. 5, pp. 773–785, May 2017.

[3] Z. Liu, D. Liu, and X. Zou, "An efficient and flexible hardware implementation of the dual-field elliptic curve cryptographic processor," IEEE Trans. Ind. Electron., vol. 64, no. 3, pp. 2353–2362, Mar. 2017.

[4]B.Parhami, Computer Arithmetic: Algorithms and Hardware Design. New York, NY, USA: Oxford Univ. Press, 2000.

[5] P. L. Montgomery, "Modular multiplication without trial division," Math. Comput., vol. 44, no. 170, pp. 519–521, Apr. 1985.

[6] S.-R. Kuang, K.-Y. Wu, and R.-Y. Lu, "Low-cost high-performance VLSI architecture for montgomery modular multiplication," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 24, no. 2, pp. 434–443, Feb. 2016.

[7] S.-R. Kuang, J.-P. Wang, K.-C. Chang, and H.-W. Hsu, "Energy-efficient high-throughput montgomery modular multipliers for RSA cryptosystems," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 21, no. 11, pp. 1999–2009, Nov. 2013.

[8] S. S. Erdem, T. Yanik, and A. Celebi, "A general digit-serial architecture for montgomery modular multiplication," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 25, no. 5, pp. 1658–1668, May 2017.

[9] R. S. Katti and S. K. Srinivasan, "Efficient hardware implementation of a new pseudo-random bit sequence generator," in Proc. IEEE Int. Symp. Circuits Syst., Taipei, Taiwan, May 2009, pp. 1393–1396.

[10] A. K. Panda and K. C. Ray, "Modified dual-CLCG method and its VLSI architecture for pseudorandom bit generation," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 66, no. 3, pp. 989–1002, Mar. 2019.