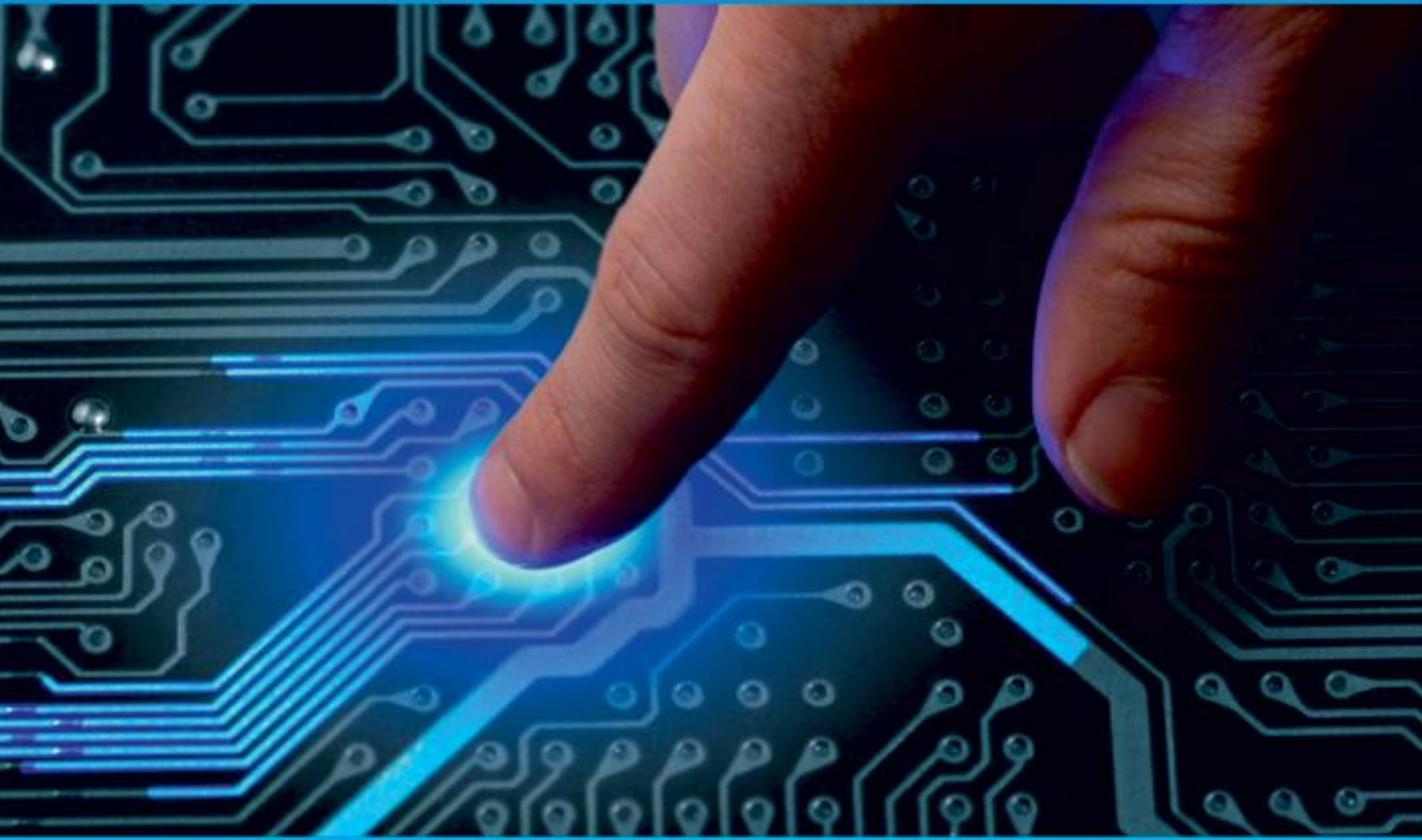
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 3, March 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103056|

DESIGN OF AREA- EFFICIENT PRBG ARCHITECTURE USING SUQARE ROOT CARRY SELECT ADDER

Y. R.K. Paramahamsa[1], N. Tejaswi[2], P. Ramya Bhargavi[3], B. Akhila[4], K. Deepthi Sai Durga[5]

Associate Professor, Department of ECE, Sri Vasavi Institute of Engineering &Technology, Nandamuru, A.P, India

U.G. Student, Department of ECE, Sri Vasavi Institute of Engineering & Technology, Nandamuru, A.P, India

U.G. Student, Department of ECE, Sri Vasavi Institute of Engineering & Technology, Nandamuru, A.P, India

U.G. Student, Department of ECE, Sri Vasavi Institute of Engineering & Technology, Nandamuru, A.P, India

U.G. Student, Department of ECE, Sri Vasavi Institute of Engineering & Technology, Nandamuru, A.P, India

ABSTRACT: Security and privacy over the internet is the most sensitive and primary objective to protect data. The data can be protected by using various cryptography and pseudorandom bit generator (PRBG) techniques. 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 is used for three-operand addition that significantly reduces the critical path delay and area of the architecture. The three-operand binary addition is thus performed using RCA logics and multiplexers, which is a novel area-efficient adder architecture that uses far less space by decreasing the number of Look Up Tables, less power, and significantly less adder delay. This proposed adder is placed in the every LCG block of MDCLG Architecture. Here, MDCLG generates a 32-bit random code. Moreover, it has a lesser area and lower power dissipation. Also, the proposed adder achieves less area than the existing three-operand adder techniques.

KEYWORDS: Cryptography, PRBG, Square Root Carry Select Adder, RCA, LCG, MDCLG.

I.INTRODUCTION

To enhance the development in VLSI, the cryptography methods must be implemented on software in order to obtain the best system performance while maintaining confidentiality. The arithmetic operations in different cryptographic methods typically involve modular arithmetic, such as modular exponentiation, modular multiplication and modular addition. As a result, the effectiveness of the congruential modular arithmetic operation depends on the cryptographic algorithm which was implemented. The Montgomery algorithm, whose key operation is based on three-operand binary addition, is the most effective method for implementing modular multiplication and exponentiation. In Linear Congruential Generator (LCG) based Pseudo-Random Bit Generators (PRBG), such as linked LCG (CLCG), modified dual-CLCG (MDCLCG), and coupled variable input LCG (CVLCG), the three-operand binary addition is also a key arithmetic operation. Smaller area and less power are becoming key design considerations for VLSI circuits in the constantly expanding electronic industry, in addition to quicker units.
Hence in order to increase the mobility and battery life of portable devices, a VLSI designer must optimise area delay and power limits. While millions of instructions per second are executed by microprocessors, operating speed is the most crucial restriction to take into account when constructing multipliers. Due to the difficulty of achieving these limitations, a compromise between them must be established depending on the application. Adder design can be done in a variety of ways.

By balancing the delay through two carry chains and the block multiplexer signal from the previous stage, the square-root carry select adder is built. Non-linear carry select adder is another name for it. An arithmetic combinational logic circuit known as a carry select adder adds two N-bit binary values and outputs the resulting N-bit binary sum and a 1-bit carry. The fundamental benefit of CSA is its characteristics of reduced propagation delay. This is accomplished by the use of parallel stages, which are produced by using many pairs of ripple carry adders. The carry input is assumed to be 0 or 1, respectively, by the ripple carry adders, who provide the intermediate sum and carry for the CSA structure.

II.EXISTING SYSTEM

In order to accomplish the three-operand addition in modular arithmetic, this section introduces a new adder technique and associated VLSI design. The adder method that is being suggested is a parallel prefix adder. To compute the addition of three binary input operands, such as bit-adding logic, base logic, PG (propagate and generate) logic, and sum logic, it has four-stage structures rather than three-stage structures in the prefix adder. The definitions of each of these four levels' logical expressions are as follows.

Stage-1: Bit Addition Logic:

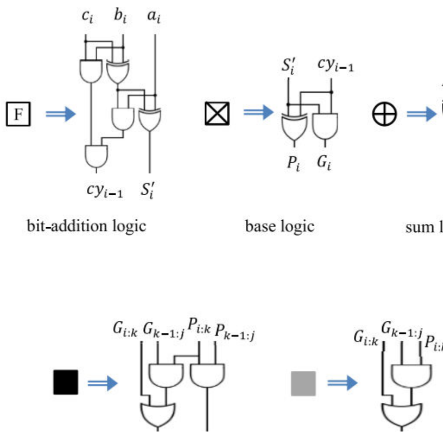
$$S_i' = a_i \oplus b_i \oplus c_i,$$
$$cy_i = a_i \cdot b_i + b_i \cdot c_i + c_i \cdot a_i$$

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

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



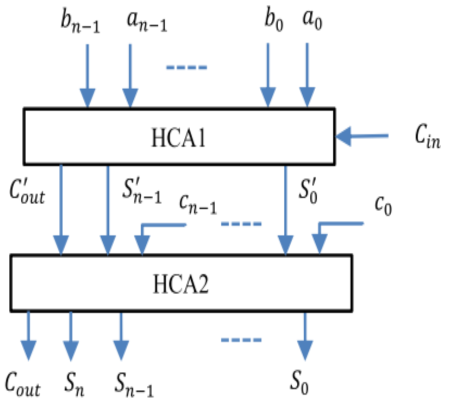
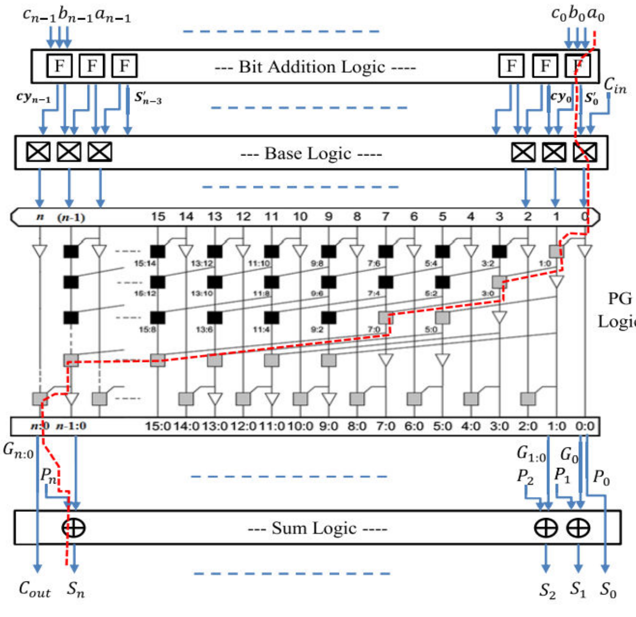

b_{n-1} a_{n-1} b_0 a_0
HCA1
C_{in}
C_{out}' S_{n-1}' c_{n-1} S_0' c_0
HCA2
C_{out} S_n S_{n-1} S_0

Fig. 2.1: Block level architecture of HCA-based three-operand adder (HC3A).


$c_{n-1}b_{n-1}a_{n-1}$
$c_0b_0a_0$
--- Bit Addition Logic ----
cy_{n-1} S_{n-3}' cy_0 S_0' C_{in}
--- Base Logic ----
n (n-1) 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
PG Logi
n:0 n-1:0 15:0 14:0 13:0 12:0 11:0 10:0 9:0 8:0 7:0 6:0 5:0 4:0 3:0 2:0 1:0 0:0
$G_{n:0}$ P_n $G_{1:0}$ G_0 P_2 P_1 P_0
--- Sum Logic ----
C_{out} S_n S_2 S_1 S_0

(a)

Fig. 2.2: Existed three-operand adder; (a) First order VLSI architecture.

The HCA-based three-operand adder's (HC3A) detailed architecture is shown in. The propagate chain, or the number of black-grey cell stages in the PG logic of the Han-Carlson adder, determines the maximum combinational path delay of the HC3A and is calculated as follows:

$$\mathrm{T_{HC3A}} \approx 4\mathrm{T_X} + 4\left\lfloor \log_2 n \right\rfloor \mathrm{T_G}$$
$$\mathrm{A_{HC3A}} \approx (4n+1)\,\mathrm{A_X} + 6\left[n + \left\lceil \frac{n}{2} \right\rceil s - 2^s + 1\right] \mathrm{A_G}$$

In comparison to the HCA-based three-operand adder (HC3A) significantly increases the area grows in the order of O with increasing bit length (n log2 n).Thus, to reduce the area in the MDCLG, we chosen the proposed adder such that is Square Root carry select adder.

III.PROPOSED SYSTEM

Two RCA blocks make up the Carry Select Adder. In this project, we suggested a square root carry select adder to shorten the ideal delay. The block size in Square Root Carry Select Adder (SRCSA) might vary. A 16-bit adder can be made utilising block sizes of 2-2-3-4-5 rather than using a uniform block size of four (as done before). The full analysis is omitted here for conciseness. When the Full-Adder delay and the MUX delay are equal, this break-up is perfect. The inputs are A and B, the carry-in is denoted as Cin, and the outputs are denoted by sum (S) and carry-out in the block diagram of the proposed SRCSA adder in Fig.3.1. (Cout).

By balancing the delay through two carry chains and the block multiplexer signal from the previous stage, the square-root carry select adder is built. Non-linear carry select adder is another name for it.
The primary drawback of conventional CSLA is the enormous space caused by the numerous pairs of ripple carry adders. The basic square-root Carry Select adder features a dual ripple carry adder with a 2:1 multiplexer. Here is a diagram of a standard 16-bit SQRT Carry select adder.

16-bit sqrt carry select adder

A 16-bit sqrt carry-select adder is divided into sectors, each of which, with the exception of the least significant, executes two additions concurrently, one assuming a carry-in of zero and the other a carry-in of one. Additionally, each sector has two 4-bit rcas that receive the same data inputs but different Cin.

One of the two adders is chosen based on the real Data from the sector before. The sum and carryout of the higher adder are chosen if the carry-in is zero. The sum and carry-out of the lower adder are chosen if the carry-in is one. Regular 16-bit SQRT CSLA has a five sets of RCAs of various sizes.

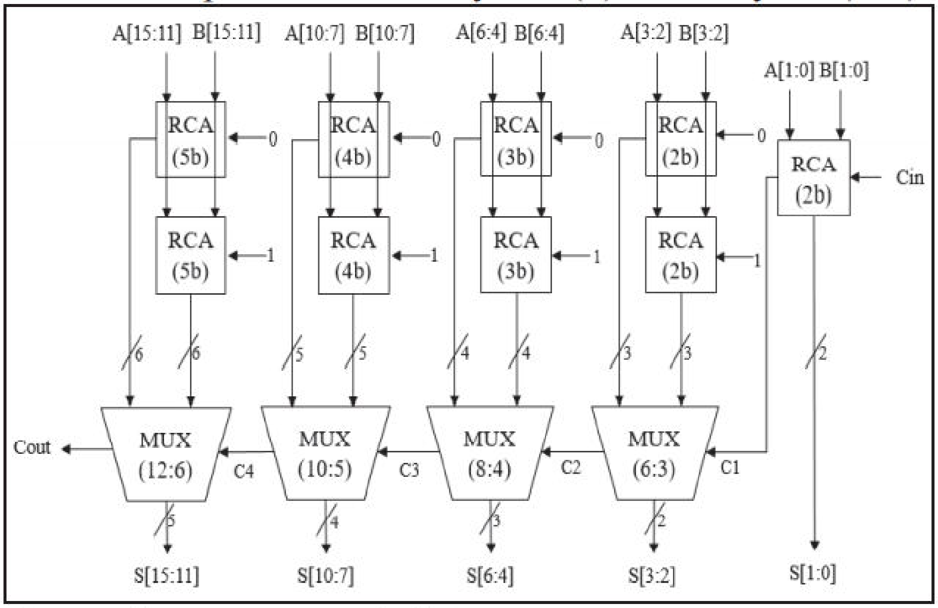


Fig. 3.1: 16-bit SRCSA (proposed adder)

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

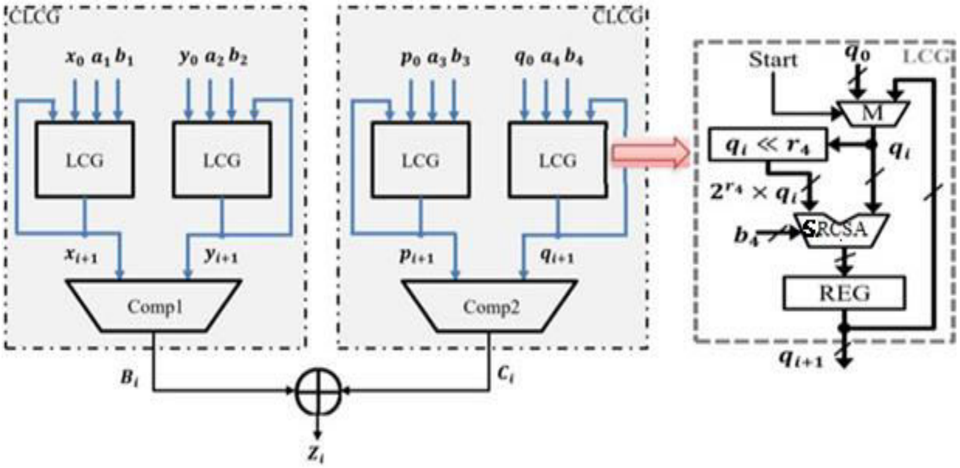
|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103056|

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

For the fastest encryption and decryption, the hardware security in the field of IoT applications requires stream-cipher based high data rate, lightweight cryptography technology. The main part of stream-cipher based encryption and decryption is the key generator, also known as the pseudorandom bit generator (PRBG). The most effective PRBG technique that is suited for hardware security based on stream cyphers is modified dual-CLCG (MDCLCG). Yet, the bit size of the congruential modulus has a linear relationship with the security strength of the MDCLCG technique. If n 32 bits, it is polynomial-time unpredictable and secure. As can be seen in Fig.3.2, the hardware design of the MDLCG approach is based on LCG, with the three-operand modulo2n adder serving as the main computational arithmetic block.
Four registers, multiplexers, a Square Root Carry Select Adder, and two magnitude comparators make up the MDCLCG design is represented in fig 3.2. The performance of the MDCLCG architecture is influenced by the amount of space utilised in the HCA together with an increase in bit size. As a result, the suggested Square Root Carry Select Adder architectures are used in this part to replace the HCA adder and measure the performance parameters of the MDCLCG. The architecture of the proposed adder is further revised to take into account the MDCLCG method's three-operand modulo-2n adding operation.

The suggested design is synthesised using a 32nm CMOS technology library that is commercially accessible. Moreover, it dissipates less power and has a smaller surface. Moreover, compared to the existing three-operand adder techniques, the proposed adder achieves less area.



4.1: 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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103056|

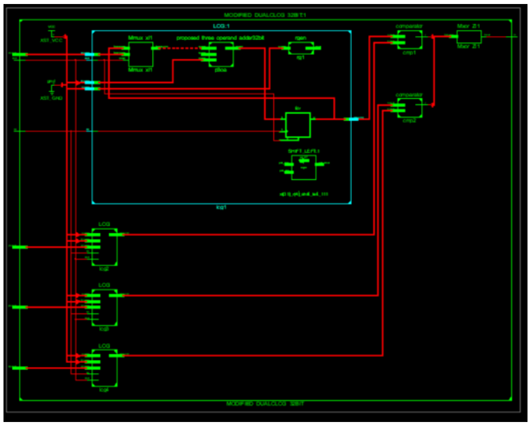


Fig 4.1.1: RTL Schematic of Existed MDCLCG

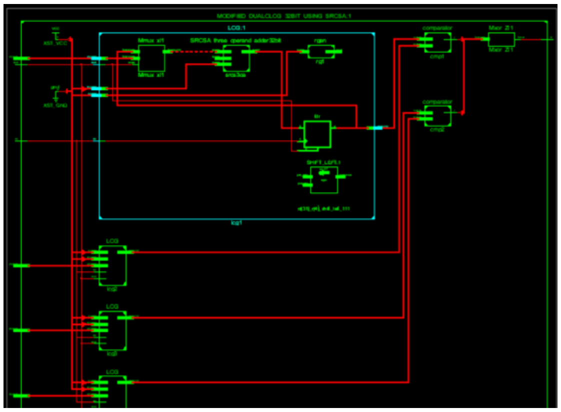
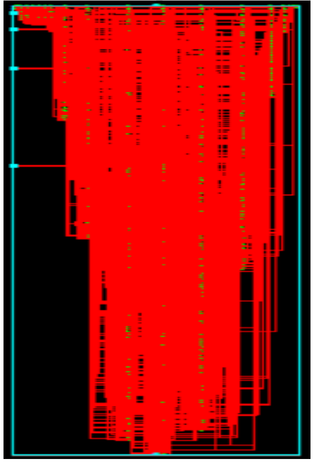

MODIFIED DUALCLCG 32BIT USING SRCSA:1
LCG:1
Mmux_xl1
SRCSA three operand adder32bit
rgen
comparator
Mxor_Z:1
SHIFT_LEFT:1
lcg1
LCG

Fig 4.1.2: RTL Schematic of Existed MDCLCG

4.2: 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.



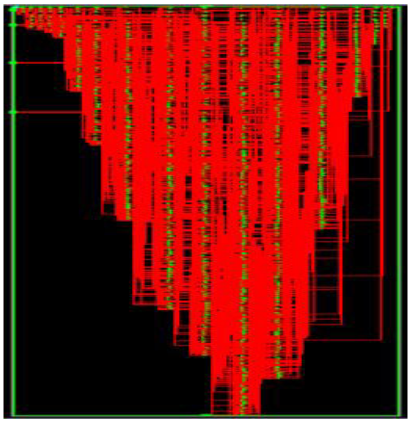
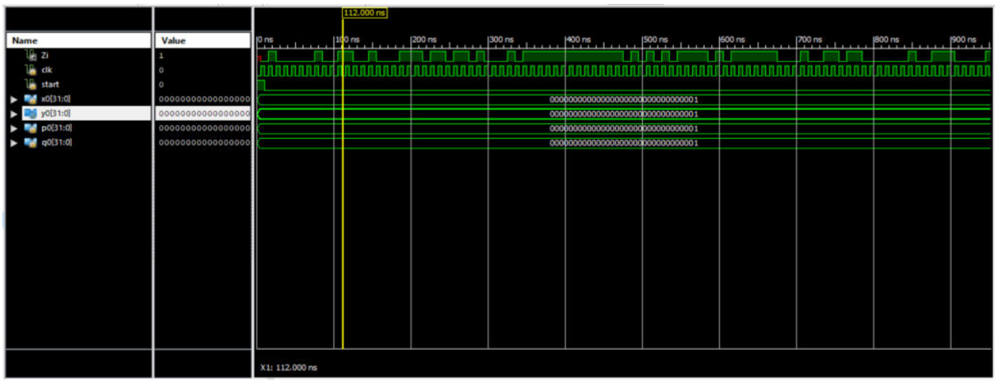


Fig 4.2.1: View Technology Schematic of existed MDCLCG

Fig 4.1.1: View Technology Schematic of proposed MDCLCG

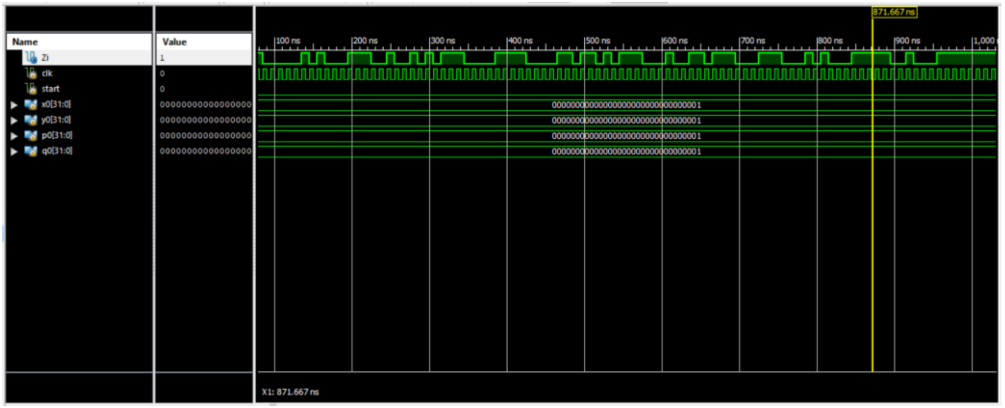
4.3 SIMULATION:



Name	Value
Zi	1
clk	0
start	0
x0[31:0]	0000000000000000
y0[31:0]	0000000000000000
p0[31:0]	0000000000000000
q0[31:0]	0000000000000000

Fig 4.3.1: Simulated Waveforms of existed MDCLCG

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 implantation to the simulation on the home screen of the tool ,and the simulation window confines the output in the form of the wave forms. Here it has the flexibility of providing the different radix number systems



Name	Value
Zi	1
clk	0
start	0
x0[31:0]	0000000000000000
y0[31:0]	0000000000000000
p0[31:0]	0000000000000000
q0[31:0]	0000000000000000

Fig 4.3.2: Simulated Waveforms of proposed MDCLCG

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 implantation to the simulation on the home screen of the tool and the simulation window confines the output in the form of the wave forms. Here it has the flexibility of providing the different radix number systems.

Parameter comparison

Parameter	Existed MDCLCG	Proposed MDCLCG
No of LUTs	715	646

Table 4.3.3: LUT's comparison

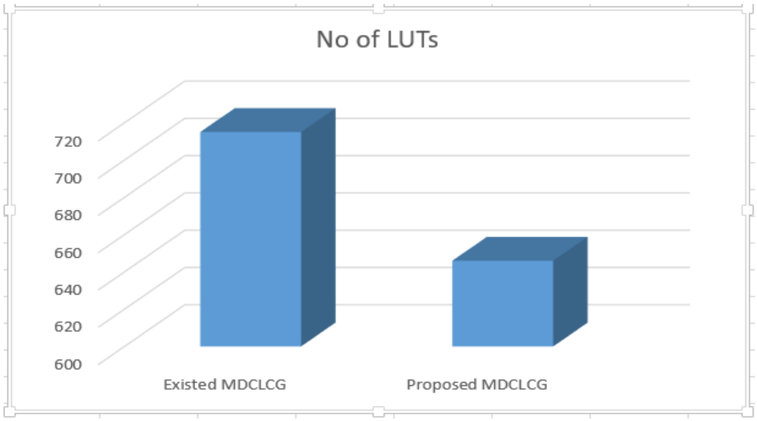


Fig 4.4.4: LUT comparison Bar graph

V.CONCLUSION & FUTURE SCOPE

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] Amit Kumar Panda , Rakesh Palisetty and Kailash Chandra Roy ,"High Speed Area Efficient VLSI Architecture of Three Operand Binary Adder", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS–I: REGULAR PAPERS, VOL. 67, NO. 11, NOVEMBER 2020

[2] 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.

[3] 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.

[4] 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.

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

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] A. Kumar Panda and K. Chandra Ray, "A coupled variable input LCG method and its VLSI architecture for pseudorandom bit generation," IEEE Trans. Instrum. Meas., vol. 69, no. 4, pp. 1011–1019, Apr. 2020.

[13] N. Weste and K. Eshraghian, Principles of CMOS VLSI Design—A Systems Perspective. Reading, MA, USA: Addison-Wesley, 1985.

[14] T. Kim, W. Jao, and S. Tjiang, "Circuit optimization using carry-saveadder cells," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 17, no. 10, pp. 974–984, Oct. 1998. [14] A. Rezai and P. Keshavarzi, "High-throughput modular multiplication and exponentiation algorithms using multibit-scan–multibit-shift technique," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 23, no. 9, pp. 1710–1719, Sep. 2015.

[15] A. K. Panda and K. C. Ray, "Design and FPGA prototype of 1024- bit Blum-Blum-Shub PRBG architecture," in Proc. IEEE Int. Conf. Inf. Commun. Signal Process. (ICICSP), Singapore, Sep. 2018, pp. 38–43.

[16] T. Han and D. A. Carlson, "Fast area-efficient VLSI adders," in Proc. IEEE 8th Symp. Comput. Arithmetic (ARITH), May 1987, pp. 49–56.

[17] D. L. Harris, "Parallel prefix networks that make tradeoffs between logic levels, fanout and wiring racks," U.S. Patent 0 225 706 A1, Nov. 11, 2004.

[18] H. Ling, "High-speed binary adder," IBM J. Res. Develop., vol. 25, no. 3, pp. 156–166, Mar. 1981.

[19] R. Jackson and S. Talwar, "High speed binary addition," in Proc. Conf. Rec. 38th Asilomar Conf. Signals, Syst. Comput., vol. 2. Pacific Grove, CA, USA, Nov. 2004, pp. 1350–1353.

[20] K. S. Pandey, D. K. B. N. Goel, and H. Shrimali, "An ultra-fast parallel prefix adder," in Proc. IEEE 26th Symp. Comput. Arithmetic (ARITH), Kyoto, Japan, Jun. 2019, pp. 125–134.

[21] F. Jafarzadehpour, A. S. Molahosseini, A. A. Emrani Zarandi, and L. Sousa, “New energy-efficient hybrid wide-operand adder architecture,” IET Circuits, Devices Syst., vol. 13, no. 8, pp. 1221–1231, Nov. 2019.
[22] S. Muthyala Sudhakar, K. P. Chidambaram, and E. E. Swartzlander, “Hybrid Han-Carlson adder,” in Proc. IEEE 55th Int. Midwest Symp. Circuits Syst. (MWSCAS), Boise, ID, USA, Aug. 2012, pp. 818–821.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details