AREA OPTIMIZED VLSI ARCHITECTURE OF MODIFIED DUAL CLCG METHOD FOR PSEUDORANDOM BIT GENERATION

Venkumahanthi Ravikiran Research Scholar, Sri Sivani College of Engineering, Chilakapalem, Andhra Pradesh 532402

Jeevan Kumar Vajja Assistant Professor, Sri Sivani College of Engineering, Chilakapalem, Andhra Pradesh 532402

ABSTRACT

The three-operand binary adder serves as the fundamental functional unit for cryptography and pseudorandom bit generator (PRBG) techniques, both of which are necessary for the performance of modular arithmetic. At the expense of extra hardware, a square root carry select adder is utilized for the addition of three operands, considerably reducing the critical route time. As a result, RCA logics presents a new design for a high-speed and area-optimizing adder to conduct To reduce the amount of area, power, and latency of the adder by doing three-operand binary arithmetic. On an FPGA device, the proposed design has been functionally tested. and generated using a 32nm CMOS technology library that is commercially accessible. It also has a lower surface area and less power dissipation. Furthermore, compared to conventional three-operand adder techniques, the proposed adder uses considerably less area.

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

I. INTRODUCTION

An adder is a digital circuit that may be used to add two numbers together accomplish the operation of adding numerical values. Adders are a kind of component that may be found in the arithmetic logic units (ALU) of many

different types of processors and computers. They are also used in other components of the CPU to compute things relating to addresses and table indexes, increment and decrement operators, and other things similar to these.

Binary numbers are by far the most prevalent kind of number format, despite the fact that adders can be made to work with many different kinds of numbers, like binary-coded decimal and excess-3. Using two's complement or ones complement to signify negative numbers turns an adder into a subtractor. These complements are called complements of two or complements of one.

The straightforward adder cannot be used for other signed number representations; further reasoning is required. The Binary Adder is another straightforward and basic combinational logic circuit that can add two or more binary values together. It is possible to build the Binary Adder using just a few straightforward logic gates.

Cryptographic algorithms must be implemented on hardware to guarantee the best possible performance of the system while keeping the physical environment safe. The operations of modular exponentiation, modular multiplication, and modular addition are all examples of modular arithmetic techniques are extensively employed in different encryption methods.

As a result, the efficiency with which the congruential modular arithmetic operation is implemented determines the performance of the cryptographic method. Critical operation of the Montgomery algorithm is using the binary addition with three operands, is the most efficient method for implementing modular multiplication and exponentiation.

There are several Pseudorandom bit generators based on linear congruential generators that make use of the three-operand binary addition as a fundamental math operation, including: the connected LCG (CLCG) [9], the linked variable-input LCG [10], and the modified dual-LCG (MDCLCG) (CVLCG) (see Figure 1). All of the modern LCG-based and other PRBG algorithms, the modified dual-CLCG, also known as MDCLCG, is the PRBG approach that is considered to be the safest and most random.

If n has 32 bits, it is unpredictable and secure in polynomial time. As a result, as operand size increases, so does the security of the MDCLCG. However, the physical design of this device consists of two comparators and four adders with three operands and modulo-2n and four multiplexers There is an increase in area and critical path time that is linear As a result.

The MDCLCG's performance may be enhanced with an Three-operand adder implementation in an effective manner One three-operand adder or two two-operand adders may be used for binary addition with three operands.

II. LITERATURE SURVEY

Katti and Srinivasan. "New hardware pseudo-random bit sequence generator" A dual-CLCG for making bits that look like they came from nowhere is shown. in this study to enhance generator speed while minimizing power consumption with the smallest possible chip footprint. To increase A unique pseudo-random bit generator (PRBG) is given that combines a two-operand modulo adder and a dual-CLCG architecture without shifting operations.

The proposed dual-CLCG architecture uses a two-operand modulo adder instead of one with three, and it doesn't need shifting. The goal of this research is to make pseudo-random bits at a constant clock rate with the highest possible clock frequency and the longest possible random bit sequence. The proposed architecture also shows power loss with the ideal chip area of PRBG. The National Institute of Standards and Technology ran 15 tests on the generated sequence, and it passed all of them.

To generate pseudorandom bits, a modified dual-CLCG technique and associated VLSI architecture were developed. K. Panda and K. C. Ray are partners in crime. Among the several LFSR, LCG, and chaotic-based PRBG techniques, the most efficient is the LFSR. the chaotic-based technique is the most efficient the dual coupled-LCG (dual-CLCG) is a safe PRBG approach. Because of the presence of inequality equations, the hardware implementation of this approach faces a bottleneck.

Initially, the dual-CLCG technique is directly architecturally mapped. It creates pseudorandom bits at different intervals using two inequality equations, resulting in a wide range of output latency. Furthermore, it uses a considerable amount of space and fails to accomplish the maximum period. To address the aforementioned shortcomings, Coupled variable input LCG (CVLCG) is an innovative, A PRBG technique that works well and its architecture are proposed.

When you connect two newly made variable-input LCGs, you get pseudorandom bits at a constant clock rate, the longest possible sequence, and less space taken up by one comparator than with a dual-CLCG design.

III. MODIFIED DUAL CLCG USING SQUARE ROOT CAARY SELECT ADDER TECHNIQUE

The suggested adder's performance is further evaluated by inserting it into The modified dual-CLCG (MDCLCG) PRBG approach provides lightweight hardware security with a high data throughput in IoT applications.

Hardware security in the sphere of IoT applications necessitates a high data rate, lightweight cryptography solution based on stream cyphers for the quickest encryption/decryption. The key generator, also known as The pseudorandom bit generator (PRBG) is the most crucial element of stream-cipher-based encryption and decryption. The most efficient PRBG algorithm suitable for stream-cipher based hardware security is modified dual-CLCG (MDCLCG).

The security strength of the MDCLCG technique is related to the bit size of the congruential modulus. If n is 32 bits, it is unpredictable and secure in polynomial time [10]. As seen in Figure 1, the MDLCG method's hardware architecture is based on LCG, with a three-operand modulo2n adder acting as the core An algorithmic calculation block. Three-operand modulo-2n adder and two magnitude comparators are part of the MDCLCG design defined in [10]. Because the conventional adder consumes more area, the MDCLCG design doesn't perform as effectively as it might. The square root carry save adder replaces the conventional adder in this part, allowing us to assess the MDCLCG's performance metrics while also offering other adder topologies. The architecture of the suggested adder is changed again to take into account how the MDCLCG method works when adding three operands modulo 2n.

SQUARE ROOT CARRY SELECT ADDER

Carry Select Adder is made up of two rca blocks. In this research, we suggested a square root carry choose adder to lower the optimum latency. The block size in Square Root Carry Select Adder (SRCSA) may be varied [9–10]. For brevity, the whole analysis is omitted here, however a 16-bit adder may be developed utilising block sizes of 2-2-3-4-5 instead of four (as previously done) [8].

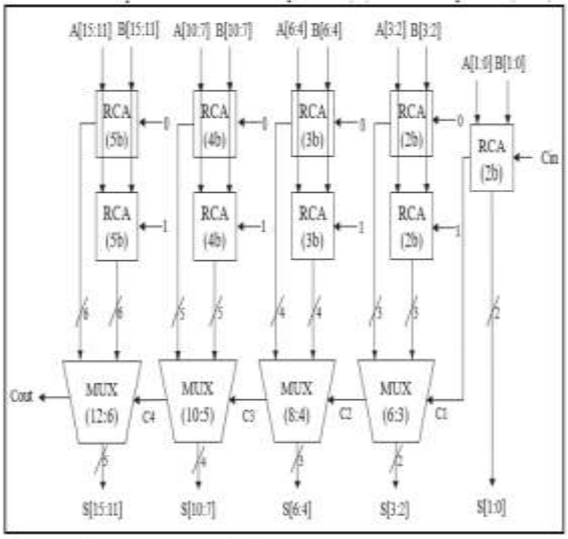


Fig. 1. 16-bit SRCSA (proposed adder)

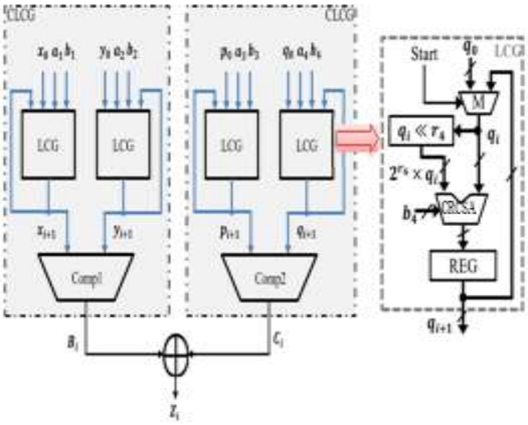


Fig.2. MDCLCG architecture Using CRCSA

IV. RESULTS

RTL SCHEMATIC:- The register transfer level (RTL) schematic denotes the architecture's blueprint and is used to compare perfect architecture that we must create from the intended architecture. The hdl language is used to transform the architecture's description or summary into the functioning summary using a coding language like verilog or vhdl. The internal connection blocks are even specified in the RTL schematic for easier analysis. Below is a schematic representation of the design's RTL implementation.

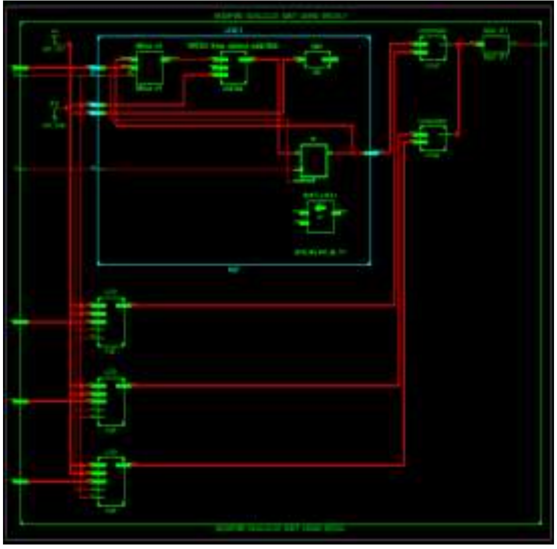


Fig3: RTL Schematic of Proposed MDCLCG

TECHNOLOGY SCHEMATIC:- With the LUT area parameter being used to estimate architecture design in VLSI, this diagram shows the technology's architecture in LUT format. The FPGA's LUTs, which are square units, represent the code's memory allocation.

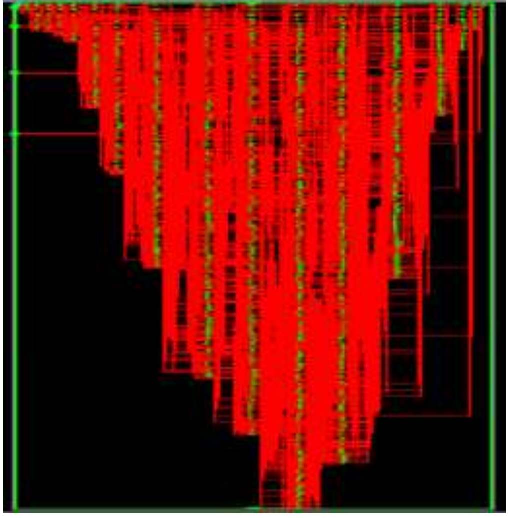


Fig4: View Technology Schematic of proposed MDCLCG

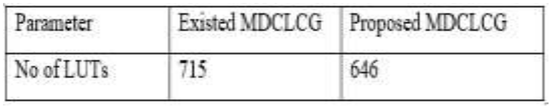
SIMULATION:-

Unlike the schematic, which only verifies the connections and blocks of a circuit, a simulation verifies the circuit's workings. Waveforms are the only form of output that can be viewed in the simulation window because it is launched by shifting from implementation to simulation. Since it can support multiple radix number systems, this is a useful feature.

Fig5: Simulated Waveforms of proposed MDCLCG

PARAMETERS:-

Consider that in VLSI, the factors considered are area, delay, and power; using these metrics It's possible to make comparisons between several designs. XILINX 14.7 is used to acquire the parameter, while verilog is used as the HDL language.



Parameter	Existed MDCLCG	Proposed MDCLCG
No of LUTs	715	646

Table1 : parameter comparison

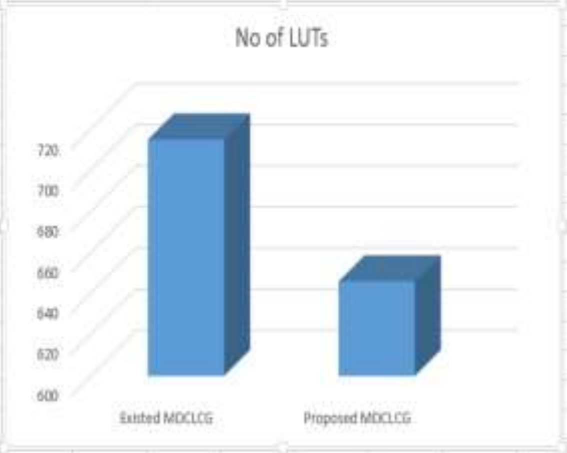


Fig6: LUT comparison bargraph

V. CONCLUSION

Due to the modified Dual-CLCG approach's dual coupling of four LCGs, the modified Dual-CLCG technique is more secure than LCG-based PRBGs. However, it has been observed that this approach has the disadvantage of producing pseudorandom bits across a broad region with higher latency. The suggested architecture of the new modified dual-CLCG technique employing square root carry chooses adder reduces the design area considerably. The improved dual-CLCG method's The proposed architecture is tested on FPGA devices that are already on the market, and validation data is collected utilising the Xilinx chip scope in real time. When it came to analysing complexity, randomness, and security of the hardware, the suggested modified dual-CLCG technique was shown to be the most effective in terms of 32-bit hardware design, 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.