Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

AN ANALYSIS OF AREA BASED THREE OPERAND BINARY ADDER VLSI ARCHITECTURE

Nimmada Chanikya Research Scholar, LENDI INSTITUTE OF ENGINEERING AND TECHNOLOGY, Jonnada (Village), Denkada (Mandal), Vizianagaram Dist – 535005
Dr.S. Sridhar Professor and controller of examinations, LENDI INSTITUTE OF ENGINEERING AND TECHNOLOGY, Jonnada (Village), Denkada (Mandal), Vizianagaram Dist – 535005

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.

Key words— Three-operand adder, square root carry select adder, modular arithmetic.

1.INTRODUCTION

Cryptographic algorithms must be implemented in hardware in order to provide the best possible system performance and assure physical security [1-3]. Modular exponentiation, modular multiplication, and modular addition are all examples of modular arithmetic utilised frequently in cryptographic procedures [4]. Thus, the cryptographic method's implementation affects congruential modular arithmetic performance. Modular multiplication and exponentiation are most efficiently implemented using the Montgomery algorithm [5-7], which employs three-operand binary addition. In linear congruential generator (LCG)-based PRBGs ,adding three binary operands is important.There is security and randomness in polynomial time if n is 32 bits. Hence, the MDCLCG strengthens with larger operand

sizes. Area and critical route time also grow linearly [10. SRCSLA can help the MDCLCG.The binary addition of three operands can be carried out using either a single three-operand adder or a pair of two-operand adders. SRCSLAis a common and efficient modular arithmetic technique for three-operand binary addition. [5-8], [9]. MDCLCG and other cryptographic algorithms suffer from CS3A's ripple-carry stage's increased carry propagation time on IoT-based hardware devices. 3 operand binary adders use Han-Carlson (HCA) parallel prefixed two-operand adders. decreasing crucial journey time. Critical route time falls by O(log2 n), while area rises by O(n log n). High-speed, compact pre-compute bitwise addition with carry-prefix is innovative. The three-operand adder based on HCA consumes significantly more energy than the compute logic used in this investigation. minimises gate size and propagation delay (HC3A). The proposed adder design also made use of a commercially available library of 32nm CMOS technology and a Verilog HDL implementation.

2.LITERATURE SURVEY

"Modular multiplication without trial division," We describe a technique to multiply two numbers (referred to as N-residues) modulo N without dividing by N. Due to the nonstandard representation of N-residues, this approach is only effective when There are various calculations completed by adjusting by a factor of N. It is still the case that addition and subtraction follow the same rules. which uses a straightforward and effective method of Montgomery multiplication (MMM). In this case, it is advised that hybrid full adders be incorporated into the CSA. The hybrid full adder is built with transmission gate logic and a regular complementary metal oxide semiconductor. Hybrid adders reduce Full-Adder power usage by 46% and 52%, respectively. SCS-based MMMs have 47% lower latency than Radix 2 MMMs. New data transmission and internet services are known to have weak and complex security issues. The employment of cryptographic algorithms is an effective means of providing safety for such infrastructures. Cryptographic systems that are implemented in hardware would prevent this. In comparison to secret-key cryptosystems, public-key cryptosystems see far heavier deployment. A fundamental operation in many public-key cryptosystems, modular multiplication is increasingly important in modern cryptographic protocols. using a lot of data as inputs. Trial and error is involved in modular multiplication.

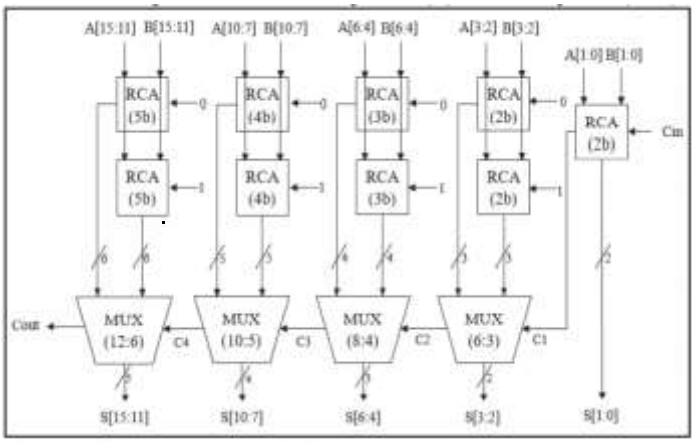
3.THE EFFECTIVENESS THE THREE-OPERAND ADDER AND THE REVISED DUAL-CLCG STRUCTURE

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

IoT hardware security requires stream-cipher-based high-data-rate, lightweight encryption. Encrypting and decrypting at the quickest rates requires this. Stream-cipher encryption and decryption use the key generator (PRBG). When it comes to stream cypher hardware security, the modified dual-CLCG method is the most effective PRBG approach (MDCLCG). Nonetheless, it has been demonstrated that the MDCLCG method's security level has a linear relationship with the size of the congruential modulus in terms of bits. Hardware implementations of LCG-based methods like MDLCG make heavy use of the three-operand modulo2n adder, as seen in Figure 4. This is due to the LCG's foundational role in the MDLCG approach. MDCLCG architecture described in [10]. The performance of the MDCLCG design is impacted by an increase in bit size due to carry propagation gate delay in the CS3A adder that was significantly longer. As a consequence of this, the HHC3A and certain recommended adder topologies are applied in this section in place of the CS3A adder so that performance metrics associated with the MDCLCG can be evaluated. The suggested adder's design has been modified to accommodate the MDCLCG technique's SRCSLA modulo-2n adding operation.

SQUARE ROOT CARRY SELECTADDER

Carry Select Adder has two RCA blocks. This project proposed square root carry selectadder to reduce latency. The block size in There is some room for variation in the Square Root Carry Select Adder (SRCSA) [9]–[10]. Rather than employing a constant block size of four, as was done in the past, it is possible to construct a 16-bit adder using 2-2-3-4-5 blocks [8]. Due to space constraints, the complete analysis will not be presented here. This break-up works perfectly when the MUX delay and the Full-Adder delay both have the same amount of time in it, A and B represent inputs, Cin represents carry-in, and S and C denote sum and carry-out, respectively.respectively. 1. (Cout).



Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

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

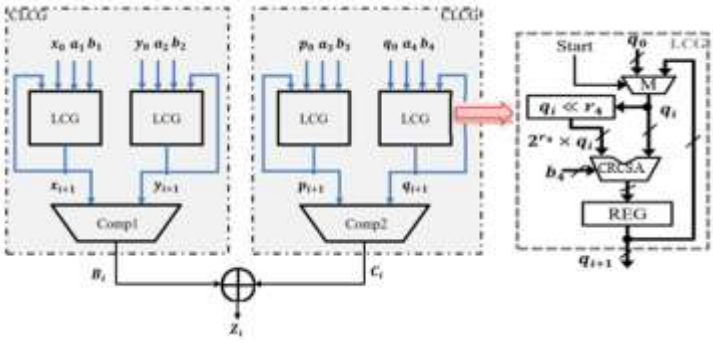


Fig. 2. MDCLCG architecture Using CRCSA

4.RESULTS

RTL SCHEMATIC:Register transfer level schematic, short for register transfer level, is the architecture's blueprint used to evaluate how closely the actual architecture comes to the ideal architectureThe computer languages i.everilog and vhdl are used to translate the architecture description, or summery, into the working summery. The internal connection blocks are also included in the RTL schematic for ease of study. The image available therein is an RTL schematic representation of the proposed architecture. below.below.

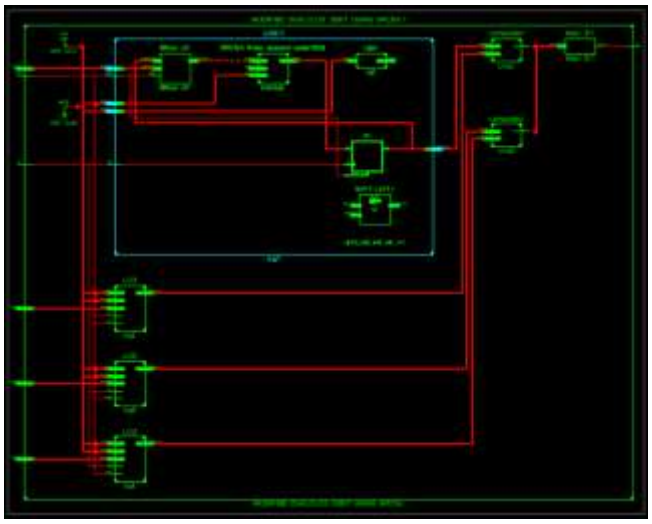


Fig3: RTL Schematic of Proposed MDCLCG

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

TECHNOLOGY SCHEMATIC: In order to estimate the area required for an architecture design in VLSI, the technology schematic produces LUT architecture image. How the programme deals with its memory allocation. represented in the LUTs of the FPGA as

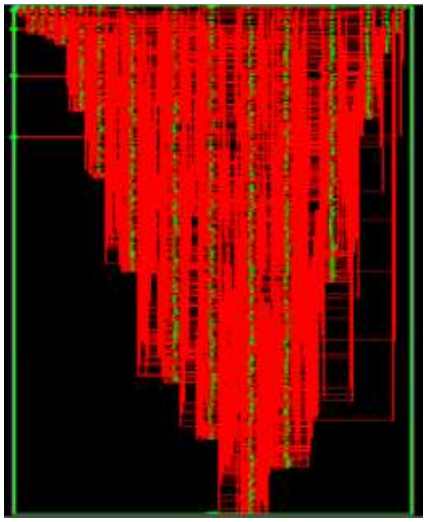


Fig4 :View Technology Schematic of proposed MDCLCG

SIMULATION: The simulation is the method that describes how it works, while the schematic is used to validate the connections and the components that make up the structure. On switching from implantation to simulation, the tool will activate the simulation window that is located on the main screen of the tool. The output is restricted to taking on the form of wave shapes by the simulation window. In this case, it is adaptable enough to offer a variety of different radix values. systems.

Fig5:Simulated Waveforms of proposed MDCLCG

PARAMETERS:Area, latency, and power are three variables that are considered in VLSI; using these variables, one can Contrast the architecture of one building with that of another. In this instance, the concept of delay is taken into consideration, Moreover, the HDL language used in this case is Verilog, and the XILINX 14.7 tool is used to derive the parameter.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

Parameter	Existed MDCLCG	Proposed MDCLCG
No of LUTs	715	646

Table 1: parameter comparison

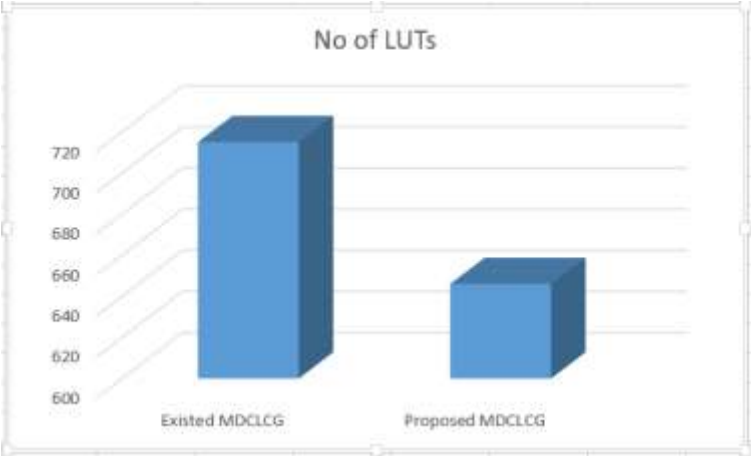


Fig6: LUT comparison bargraph

CONCLUSION

When compared to LCG-based PRBGs, the Modified Dual-CLCG technique offers a higher level of protection due to its utilisation of dual coupling of four LCGs. This approach generates pseudorandom bits across large regions and takes longer. The MD-CLCG technique with SRCSLA reduces design space. The new dual-CLCG approach's architecture is prototyped on commercial FPGA devices and validated in real time using Xilinx chipscope. Based on hardware complexity, randomness, and security, the suggested modified dual-CLCG method's 32-bit hardware architecture is best. This design may benefit hardware security, IoT, 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.