DESIGN OF128-bit ALU TO OVERCOME REVERSE ENGINEERING THEFT

PAVAN KUMAR ELISETTY
Department of Electronics and Communication EngineeringAndhra Loyola Institute of Engineering and Technology
Vijayawada, Andhra Pradesh, India

VENKATA SAI BRAHMENDRA KUMAR
Department of Electronics and communication Engineering
Andhra Loyola Institute of Engineering and Technology
Vijayawada, Andhra Pradesh, India

PAVAN KUMAR KODALI
Department of Electronics and Communication Engineering
Andhra Loyola Institute of Engineering And Technology
Vijayawada, Andhra Pradesh, India

ANANTH KUMAR PENIPOTHU
Department of Electronics and Communication Engineering
Andhra Loyola Institute of Engineering And Technology
Vijayawada, Andhra Pradesh, India

ANJANEYULU NALLURI
Asst,Prof.Department of Electronics and Communication EngineeringAndhra Loyola Institute of Engineering and Technology
Vijayawada, Andhra Pradesh, India

Abstract-**Arithmetic Logic Units are one of the crucial components in VLSI systems and it is a key element of digital processors like microprocessors microcontrollers, C.P.U. In this digital world, technology depends on the operations of A.L.U to decide the system performance. At the same time Multiplier and accumulator unit (MAC) which forms an important part of an A.L.U is the vital component in many DSP applications involving multiplications & accumulations & inner products. In this project, it has demonstrated an optimized high performance A.L.U through the use of an efficient M.A.C unit whose operations are critical in A.LU. The design consists of 128- bit ALU with Modified Wallace multiplier, 128 bit carry save adder in which is realized in VERILOG HDL and synthesized through Xilinx.**

Keywords-Design for security, Hardware Security, Logic Obfuscation, ALU, VHDL, FPGA.

1.INTRODUCTION

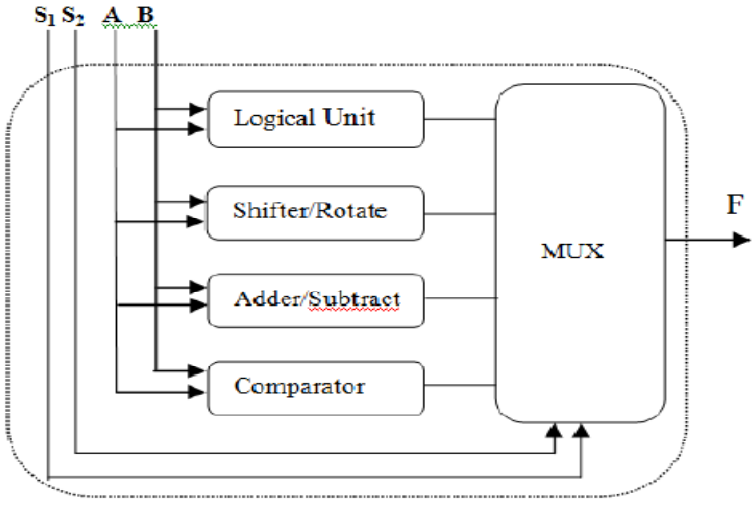
An arithmetic logic unit (ALU) is a digital circuit that performs arithmetic andlogical operations. The ALU is a fundamental building block of the central processing unit (CPU) of a computer, and even the simplest microprocessors contain one for purposes such as maintaining timers. Most ALUs can perform the following operations:

- Bitwise logic operations (AND, NOT, OR, XOR).

• Integer arithmetic operations (addition, subtraction, and sometimes multiplication and division, though this is more expensive).

• Bit-shifting operations (shifting or rotating a word by a specified number of bits to the left or right, with or without sign extension). Shifts can be seen as multiplications and divisions by a power of two. The processors found inside modern CPUs and graphics processing units (GPUs) accommodate very powerful and very complex ALUs; a single component may contain a number of ALUs. Mathematician John von Neumann proposed the ALU concept in 1945, when he wrote a report on the foundations for a new computer called the EDVAC. Research into ALUs remains an important part of computer science, falling under Arithmetic and logic structures in the ACM Computing Classification System.

A 64-bit ALU implemented using VHDL and verified on Xilinx ISE simulator. The approach used here is to split the ALU into three modules, one Arithmetic, one Logic and one Shift module. The arithmetic, logic and shift units can be combined into ALU with common selection lines. The shift micro-op operations are often performed in a separate unit, but sometimes the shift unit made part of overall ALU. For 64-bit ALU, 4:1 MUX is needed to perform particular operation. These operations arithmetic, logic, shift operation is selected according to the selection inputs. The final output of the ALU is determined by the set of multiplexers with selection lines.



fig;internal Architecture of ALU

Arithmetic Unit

Employing fast and efficient adders in arithmetic logic unit will aid in the design of low power high performance system. Other operations such as subtraction and multiplication also employ addition in their operations, and their internal hardware is almost similar though not identical to addition hardware. Various adder families have been

proposed in the past to trade-off power, area and speed for possible use in ALUs. The performance criticality of the ALU demands a dynamic adder implementation. Dynamic logic family of adders are the most efficient in terms of transistor-count, speed and power dissipation. This work covers the design of
3 bit adder using Complementary logic. This same Adder unit is used for the implementation of subtractor unit. This reuses the current hardware we made for adder and saves area.

Logic Unit

ALU can perform various logic operations like NOT, AND, OR, NAND, NOR, XOR, XNOR etc. For these operations a special unit is made called as Logical Unit. This Logic Unit performs all logic operations asked to perform. A MUX operated by select lines, for which particular logic operation to perform, is used inside this logic block.

Comparator & Shifter unit

A 1-bit comparator is made with the help of Complementary logic. It compare the two I/Ps and give three states of O/P for three different conditions. Also a 2:1 MUX is made which is used as a cell in the barrel shifter. Used for shifting and rotating operation.

Reverse Engineering Theft:

Reverse engineering, sometimes called back engineering, is a process in which software, machines, aircraft, architectural structures and other products are deconstructed to extract design information from them. Often, reverse engineering involves deconstructing individual components of larger products. The reverse engineering process enables you to determine how a part was designed so that you can recreate it. Companies often use this approach when purchasing a replacement part from an original equipment manufacturer (OEM) is not an option.

2.PROPOSED SYSTEM

In this system,we perform both Arithmetic operation And Logicaloperation and it also contain MAC unit which is useful for DSP operations.We are going to encrypt the full adder initially, because the whole components are designed with full adder. To provide security to our ALU from reverse engineering theft we must encrypt the full adder.The encryption is done with the help of key gates(k0,k1). The full adder is designed with half adder along with key gates. With the help of encrypted full adder we design 128-bit adder,64-MAC unit,and wallace tree multiplier .

The operation of 128-bit ALU is shown in the table1. If the selection line s = 0 the ALU performs addition operation between A and B operands .Similarly, if the selection line s = 1 the ALU performs subtraction operation between A and B operands.Similarly, if the selection line s = 2 the ALU performs comparator operation between A and B operands.Similarly, if the selection line s = 3 the ALU performs multiplication operation between Ap and Bp operands.Similarly, if the selection line s = 4 the ALU performs MULTIPLIER AND ACCUMILATOR operation between Am and Bm operands.Similarly, if the selection line s = 5 the ALU performs logical AND operation between A and B operands.Similarly, if the selection line s = 6 the ALU performs logical or operation between A and B operands.Similarly, if the selection line s = 7 the ALU performs logical not operation of A operand.

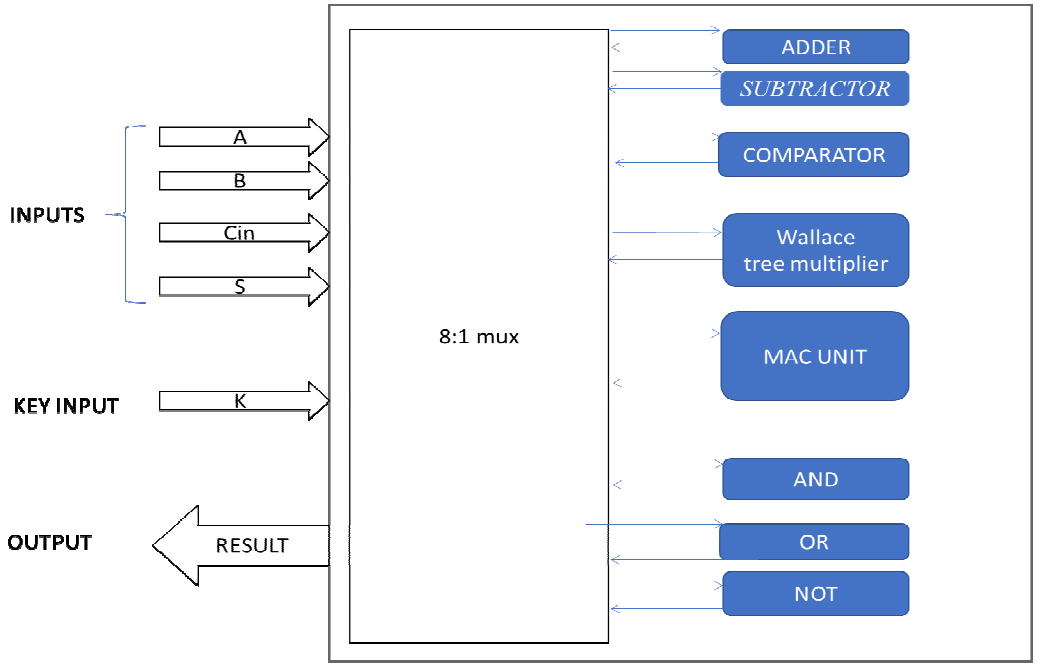


FIG:proposed ALU

S2	S1	S0	FUNCTION
0	0	0	ADDITION
0	0	1	SUBTRACTION
0	1	0	COMPARATOR
0	1	1	WALLACE TREE MULTIPLIRER
1	0	0	MAC UNIT
1	0	1	LOGICAL AND
1	1	0	LOGICAL OR
1	1	1	LOGICAL NOT

Table; operation of ALU

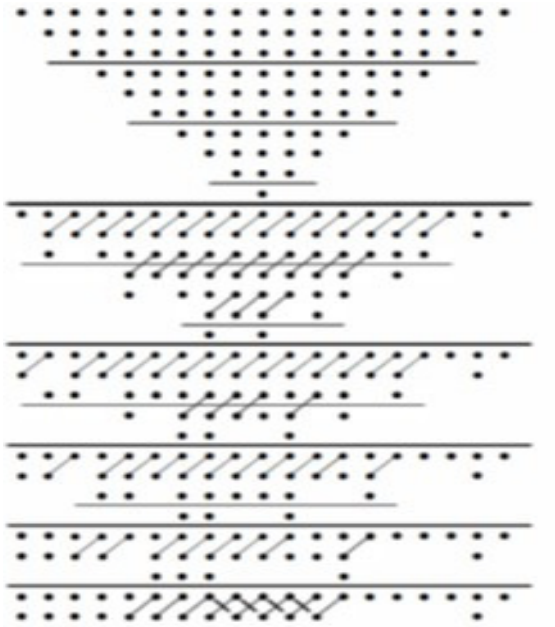
A modified Wallace multiplier:

A modified Wallace multiplier is an efficient hardware implementation of digital circuit multiplying two integers and addition using carry save compressors. Basically in conventional Wallace multipliers many full adders and half adders are used in their reduction phase, but problem with the half adders is they do not reduce the number of partial product bits. So, by minimizing the number of half adders

used in a multiplier reduction will reduce the complexity. The modified reduction method drastically reduces the number of half adders with a very slight increase in the number of full adders. Reduced complexity Wallace multiplier reduction consists of three stages.

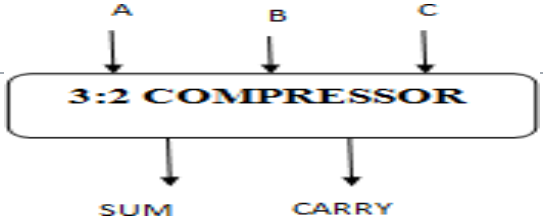
1.First Stage: The N x N product matrix is formed and before the passing on to the second phase the product matrix is rearranged to take the shape of inverted pyramid.

1. **Second Stage :** During the second phase the rearranged partial product matrix is grouped into non-overlapping group of three as shown in the figure 2, but the single bit and two bits in the group will be passed on to the next stage and three bits are given to a full adder. The number of rows in the in each stage of the reduction phase is calculated by the formula:- :- ri+1= 2(ri/3) +ri mod3 (1) if rimod3=0 ,then ri+1= 2(ri/3)



If the calculated from the above equation for number of rows in each stage in the second phase and the number of rows that are formed in each stage of the second phase does not match, only then the half adder is used.The final product of the second stage will be in the height of two bits and passed onto the third stage.

3. Third Stage: During the third stage the output of the second stage is given to the carry propagation adder to generate the final outputC.Carry Save Adder A carry save adder contains full adders which computes a single sum and carries bit based mainly on the respective bits of the three input numbers. Carry save adder is popularly known as Carry Save compressor or 3:2 counter as it counts the number of bits and sets the output result. The number of half adders are reduced in the partial product addition stage of the multiplier and they are replaced by the various compressors like 3:2, 4:2,5:2 in the reduction phase. The reason behind using compressors especially 3:2, 4:2 are due to less



critical path. The concept of Multi-Operand Addition using redundant adders is implemented by the use of higher order compressors

CARRY SAVE ADDER

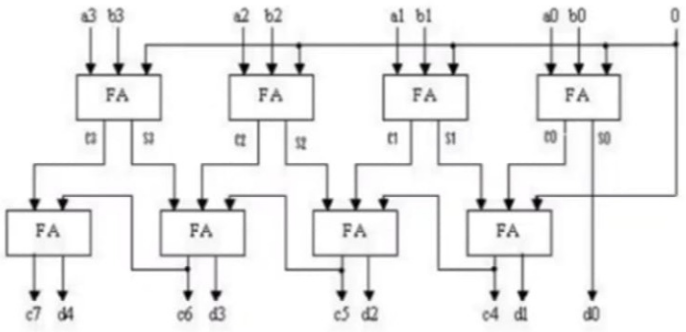


Fig:Carry Save Adder

In this design 128 bit carry save adder [6] is used since the output of the multiplier is 128 bits (2N). The carry saveadderminirnizetheadditionfrom 3 numbersto2 numbers. Thepropagationdelayis3 gatesdespiteof thenumberof bits. The carry save adder contains n full adders, computing a single sum and carries bit based mainly on therespectivebitsof thethreeinputnumbers. Theentiresum canbecalculatedbyshiftingthecarrysequenceleftbyoneplaceandthenappendinga0tomostsignificantbitof the partial sum sequence. Now the partial sum sequenceis added with ripple carry unit resulting in n + 1 bit value. The ripple carry unit refers to the process where thecarryoutofonestageisfeddirectlytothecarryinofthenextstage.Thisprocessiscontinuedwithout addingany intermediate carry propagation. Since the representation of 128 bit carry save adder is infeasible , hence a typical 8bitcarrysaveadder isshowninthe figure 3[6].Here we arecomputingthe sum of two128 bit binary numbers, then128 half adders at the first stage instead of 128 full adder. Therefore , carry save unit comprises of 128 half adders,eachofwhichcomputessinglesumandcarrybitbasedonlyonthecorrespondingbitsofthetwoinputn umbers.Ifxandyaresupposedtobetwo128bitnumbersthenitproducesthepartialproductsandcarryasSand Crespectively.Si =xi1\yi

Ci=xi&yi

Duringthe additionof twonumbersusinga half adder, two ripple carry adder is used. This is due the fact that ripplecarryadder cannotcomputeasum bitwithout waiting for the previouscarry bit to be produced, and hence the delaywill beequal tothatofnfull adders.Howevera carry-save adder producesall the output valuesin parallel, resultinginthetotal

computationtimelessthanripplecarryadders. So, Parallel In Parallel Out (PIPO) is used as anaccumulatorinthefinalstage.

MAC UNIT:

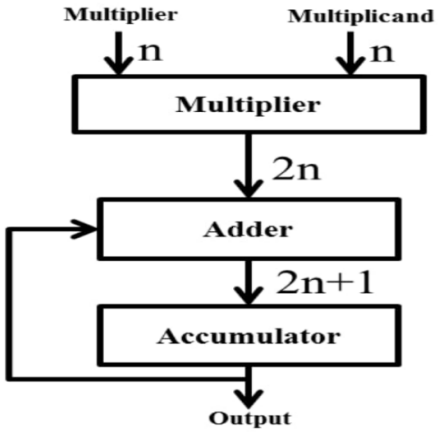


Fig:Comparator

Multiply-Accumulate (MAC) unit isextensively used in microprocessors and digital signal processors for data-intensive applications, suchasfiltering, convolution, FFT transform andinner products. [10] Because they arebasically accomplished by repetitive application of multiplication and addition, the speed of the multiplication andadditiondetermines the execution speed and performance of the entire computation. As the multiplier exhibitsinherentlylongdelayamong the basic operational blocks in digital system, the multiplier determines the criticalpath.

In order to improve the speed of the MAC unit, there are two major bottlenecks. The first is the partial productsreduction network that is used in the multiplication block and the second is the accumulator. Both of these stagesrequire addition of large operands that involve long paths for carry propagation. The main key to the proposedarchitectureisusingtheVedicmultipliertodesigntheMACunitandcomparetheperformance with theconventional MAC unitsUsingBoothMultiplier, WallaceMultiplier intermsof area, speedandnumber ofresources.

3.Encryptionlogic:

An*n*-bitALUisdesignedusingstructural modellingwhich extends the flexibility and reusability of the circuitmaking the ALU more generalized. The generalized n-bitALU is encrypted by developing an encryption logic to amodule with more connections and impact on the next levelcircuit,thataffectsmostoftheoutputs.Thishelpsindetermining which node has higher contribution or impacton the output.These nodes are identified to be the criticalnodesandkeygatesareinsertedinit.Everysub-modules of theALU comprisesfull adder in common except thecomparator.Thus,the encryption of the ALU is manifestedinthefulladder.Fulladderisbuiltof2halfaddersand1 OR gate.Sum and carry are the output of half adder.Thuswe are going to encrypt the sum and carry of the 1st halfadder byintroducing2 key gates, key gate 1 (KG1) andkey gate 2 (KG2) as shown in Fig.3 andthe encryptionlogic of KG1 and KG2 are given in Table 2 and Table 3respectively.

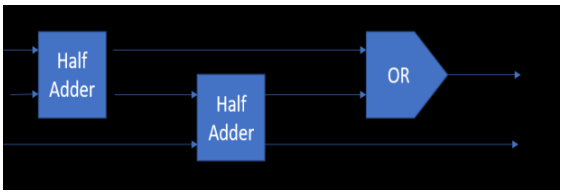


Fig.1.4.2.:FullAdder

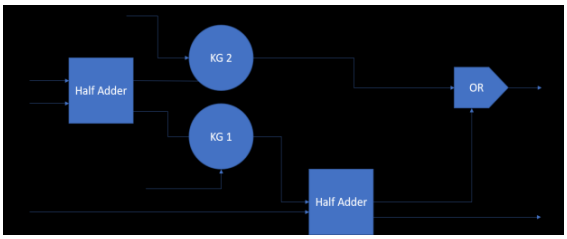


Fig.1.4.3:EncryptedFullAdder

TABLE2

ENCRYPTIONLOGICFORKG1

S_1	K_0	O_1
0	0	$\overline{\square}$
0	1	S
1	0	$\overline{\square}$
1	1	S

TABLE3

ENCRYPTIONLOGICFORKG2

C_1	K_1	O_2
0	0	C
0	1	$\overline{\square}$
1	0	C
1	1	$\overline{\square}$

As every sub modulesof the ALU comprises full adder,theinputscannotescapetheencryptionforwhateverselectionlines(S_1S_0).Thus, the outputs are affected based on the key

given.Thislogicisdesignedsothatitgivesthecorrectoutputonlyforthecorrectkeygiven.Anotheradvantagegainedbypreventingtheadversaryfromreverseengineeringthelogic.An adversary may not be aware of the key input andprimaryinputsoftheCUT.Thiswillpreventlogictheft.

4.RESULT AND ANALYSIS

The encrypted ALU is given 2 bit key as input and the output is tested for different inputs for all 4 combination of key(K1K0). The selection line inputs (s2s1s0) determines the function of the ALU and the key inputs (K1K0) determines the correctness of the result. The output is correct only for the correct key "K1K0 = 01".For wrong key combinations the output deviates much from the required output thereby perplexing the adversary

A.Functional Verification

In Fig,the inputs A,B,Cin are given values 296,296,1 respectively.For the given selection line S2S1S0= 000, the output Result holds the value of YADD = 293. These inputs are tested for all 4 combinations of key inputs K1K0 = 00,01,10,11 in regions 1,2,3 and 4 respectively.which gives different outputs for different keys out of which the outputs are correct only in region 2 where the key input K1K0 = 01.

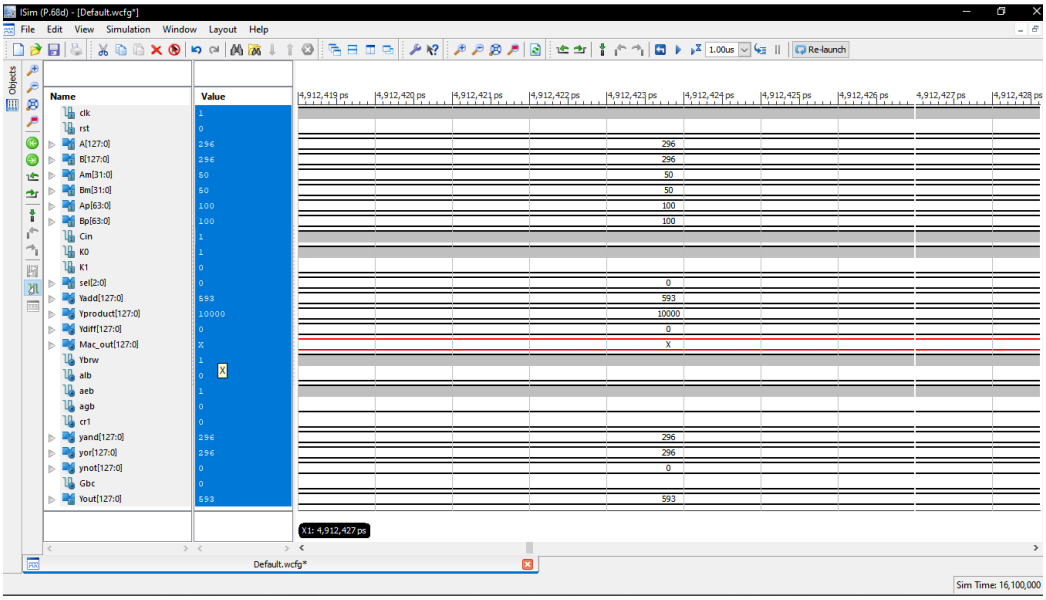


FIG: Simulation output for 128 bit ALU

The RTL schematic of ALU is shown in below figure

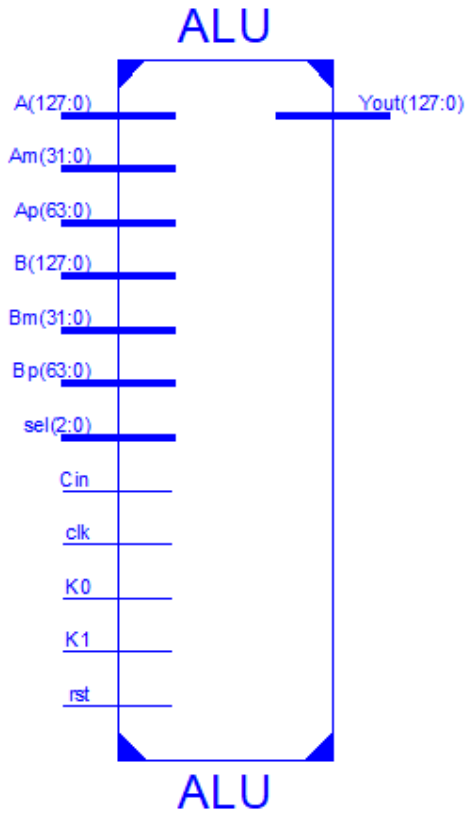


Fig: RTL schematic of ALU

B. Device utilisation analysis:

PARAMETER	EXISTING SYSTEM	PROPOSED SYSTEM
TOTAL TIME	69.374ns	65.791ns
DELAY	69.374ns	152.098ns
MEMORY	4613292KBYTES	4689652KBYTES

5.CONCLUSION

In this work" Design And implementation of a 128-bit ALU" on Xilinx using VHDL language that will perform all arithmetic operation ,logical operation ,and shifting operation .Arithmetic operation will perform operation like Addition ,subtraction ,multiplication ,division .A logical operations that are AND, OR, XOR, NOT etc. .A shift operation that is right shifting and left shifting also perform. ALU is the core of the processor and optimizing ALU can significantly improve the performance of a processor. An efficient 128-bit Arithmetic and Logic unit is successfully designed, simulated and optimized in terms of area and power using modified Wallace multiplier and carry save compressors. The A.L.U is synthesized using VERILOG HDL and successfully. The 128 bit ALU is designed and synthesized using Xilinx ise and targeted to Spartan device. The ALU is a major component of the CPU(Central Processing Unit). It performs arithmetic computation such as Addition, Subtraction, Comparator, Overflow and all basic logical operations (AND, OR, NOT, NOR, XOR, XNOR, NAND). We have verified the results obtained from Xilinx ISE Design Suit v9.1i with the

theoretical results for all the operations that were performed and found that they match with the theoretical values. The behaviorally modelled 4 bit ALU is extended to a structurally modelled n-bit ALU improving its flexibility and reusability of individual sub-circuit modules. The designed ALU is secured by implementation of an encryption logic at the fundamental sub-circuit module in common for all the higher level modules having a greater influence on the output making the encryption much.The encrypted ALU is given 2 bit key as input and the output is tested for different inputs for all 4 combination of key(K1K0). The selection line inputs (S2S1S0) determines the function of the ALU and the key inputs (K1K0) determines the correctness of the result. The output is correct only for the correct key "K1K0 = 01".For wrong key combinations the output deviates much from the required output thereby perplexing the adversary.

PARAMETER	EXISTING SYSTEM	PROPOSED SYSTEM
TOTAL TIME	69.374ns	65.791ns
DELAY	69.374ns	152.098ns
MEMORY	4613292KBYTES	4689652KBYTES

REFERENCES

[1] Gokulanathan, Sumathi. (2016). "IP Attacks and Protection Taxonomy: Logic Obfuscation as Solution".

[2] S. M. Awan, S. Rashid, Mingze Gao and G. Qu, "Functional obfuscation of digital circuits using observability don't care conditions," 2016 IEEE International Conference on Information and Automation for Sustainability (ICIAfS), Galle, 2016, pp. 1-6.

[3] Reddy D.M., K.P. Akshay, R. Giridhar, S.D. Karan and N. Mohankumar . BHARKS: Built-in Hardware Authentication using Random Key Sequence. In 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan 2017, on pp. 200– 204

[4] Chandini B., Nirmala Devi M. "Analysis of Circuits for Security Using Logic Encryption". In: Security in Computing and Communications. SSCC 2018. Comunications in Computer and Information Science, vol 969. (2019)

[5] Javier Hormigo, Julio Villalba, Member, IEEE, and Emilio L. Zapata "Multi-operand Redundant Adders on FPGAs"IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 10, OCTOBER 2013

[6] Shruti murugai and ashutosh mukerjee "ENERGY EFFICIENT AND HIGH PERFORMANCE 64 BIT ALU USING 28nm TECHNOLOGY",IEEE,2015

[7] S.Nagaraj,Dr.G.M.SreeramaReddyandDr.S.ArunaMastani;AComparative Study on Different Multipliers-SurveyJournal of AdvancedResearch in Dynamical and Control Systems14739-7522018Institute ofAdvancedScientificResearch.

[8] S. Nagaraj,K.Venkataramana Reddy and and P.Anil Kumar3i;Analysisof Vedic Multiplier for Conventional CMOS & Complementary PassTransistor Logic(CPL) Logics SCOPUS Indexed Springer 8th Interna-tional Conference on Innovations in Electronics and CommunicationEngineering,(ICIECE-2019)

[9] S.Nagaraj, B.Babu Rajesh, K.Chaithanya, P.Pratap; SIMULATION OFLOW POWER 9T & 14T FULL ADDER WITH REDUCED NOISE,Journal of Advance Research in Dynamical and Control Systems ISSN1943-023x12special2017.