JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DESIGN OF LOGICALLY SECURED ALU USING QCA TECHNOLOGY

Subtitle: DESIGN OF LOGICALLY OBFUSCATED N-BIT ALU FOR ENHANCED SECURITY

Ms.Guntamadugu Afrin, Research Scholar, Department of ECE, Viswam Engineering College (JNTUA),Madanapalli, Chittor(dist), AP, India.
afrin786413@gmail.com
Mrs.P.Hemalatha , Assistant professor, Department of ECE, Viswam Engineering College,Madanapalli, Chittor(dist),AP,India.
hemaece40@gmail.com
Mr.N.Nagendra ,Assistant professor , Department of ECE, Viswam Engineering College, Madanapalli,Chittor(dist),AP, India.
nnagendra1993@gmail.com

ABSTRACT

In digital era A.L.U. methodologies are utilised to evaluate system performance. Due to the fact that the Arithmetic Logic Unit (ALU) is a necessary component of any Central Processing Unit, its significance is equivalent to that of the computer (CPU). Due to the rarity of devices lacking an ALU, ALU encryption is crucial for the security of the device. This article covers the design of an n-bit ALU using the HDL hardware description language to maximise the flexibility and reusability of the device. In addition, by utilising quantum dot cellular autumn, the maximum efficiency of the device and the logic of obfuscation used to enhance security without compromising operation are offered. Xilinx verifies and analyses the findings, indicating that the addition of the obfuscation module has no significant impact on the amount of space or power

consumption of the ALU implemented in VERILOG HDL and synthesised by Xilinx.

Keywords: Encrypted ALU, QCA, Vedic multiplier, ripple carry adder, subtractor and comparator.

1. INTRODUCTION

The current state of remarkable chip size reduction coupled with an increase in the number of circuits on chips has led to a significant increase in battery-operated and power-sensitive applications, culminating in a boom in the emerging area of Low Power Electronics. We are interested in reducing static power at the architectural level since it ultimately determines the overall amount of power dissipated in SOCs (System on Chip). To maximise static power dissipation, we recommended synthesising the POWER GATING pproach, specifically the Fine Grain method. When the inputs of the gates are not in use, they are blocked using NMOS, which reduces input utilisation waste and significantly reduces power consumption. Consequently, the fundamental objective of our research is to minimise static power at the architectural level while simultaneously reducing power consumption, beginning with 1 bit and advancing to 8 bit.

Any digital system that lacked a processor would be useless. The ALU is a crucial microprocessor component. As a basic illustration, the ALU acts as the brain of the CPU, whereas the CPU serves as the brain of any system. Consequently, it serves as the computer's brain. They have a complex design and are composed of rapid dynamic logic circuits. CPUs utilise the great majority of a processor's total power. The ALU is one of the CPU components with the highest power density due to its near-constant operation at full speed, resulting in thermal hotspots and enormous temperature gradients. ALU designs with low peak and average power consumption and good performance. [1,2] For an ALU, an example of an A [31:0] & B [31:0] pair for a 32-bit operand pair is A [31:0] & B [31:0]. It is presented the internal architecture of a 32-bit ALU.

In this project, the encrypted alu module is developed utilising QCA technology. The Quantum-dot Cellular Automata (QCA) paradigm is fundamentally distinct from the CMOS-based paradigm because to distinctive physical phenomena and innovative approaches. Figure 1 depicts the basic component of QCA, the QCA cell, which consists of two electrons and four quantum dots. (a). P=+1 for logic "1" and P=-1 for logic "0" are the two potential polarizations utilised to encode binary information in QCA technology. Several cell topologies may be employed to generate QCA devices. Figure 1 depicts two examples of QCA cables: a binary cable and an inverter chain. (b). As seen in Figure 1(c), the binary signal spreads from input to output in a QCA wire due to electrostatic interactions between the cells, which are typically arranged so that only their corners make contact. Figure 1(d) depicts the QCA majority gate, which performs the following functions:

Y(A,B,C) = AB+BC+AC.

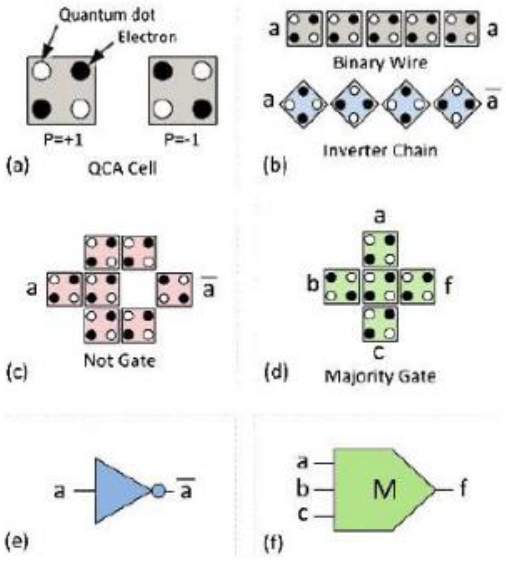


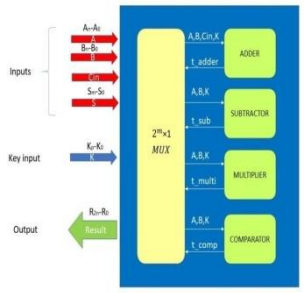
Fig1: QCA basic components.

2. LITERATURE SURVEY

Before an IC/IP can be sold, it must pass through numerous steps. The IP is built in software (.hdl), firmware (net list), and hardware (FPGA bit stream) before being sent to the system integrator, while the IC is developed and forwarded to the fabricator. Because the design must be supplied to a fabricator or system integrator in order to be executed on hardware, the original creators forfeit sole ownership. As a result, the design's functioning has been changed, resulting in a rise in design piracy and a huge loss for the electronics industry. A system can be characterised in several ways, ranging from silicon through the whole ASIC and logic gates to IP. Any of these methods might give an adversary with the chance to comprehend a design. Hardware Numerous key challenges to the design include Trojans, reverse engineering, theft, and counterfeiting. Reverse engineering may be employed to unlawfully duplicate circuit designs and steal intellectual property (IP). Because programmable components (PCs) like as RAMs may have their contents altered after an IC is constructed, according to Baumgartner, their adoption helps prevent reverse engineering. In contrast, using a PC will slow down the process since an additional mask layer is required. We feel obligated to implement encryption logic [4] to protect our n-bit ALU.

3. ENHANCED SECURITY BASED DESIGN OF LOGICALLY OBFUSED N- BIT ALU

Numerous investigations into system security have been conducted. In addition to enhancing system performance, security is a growing problem due to hardware Trojans and design theft, both of which require immediate attention. As noted above, several attempts have been made to alter the functionality of a device by installing Trojans. External circuits penetrate our intended circuit and alter its operation, so altering the circuit's only function



and posing a grave threat to the electronic hardware industry. Encryption and logic obfuscation are necessary for safeguarding the ALU against duplicate and overproduction. The inclusion of a few more circuits to the design conceals ALU functionality from unauthorised users, meaning that the right functionality is only displayed to the user who inputs the appropriate keys, which are only shared with authorised users.

The efficiency of the ALU is governed by its VLSI characteristics. To encrypt a circuit, the ALU must employ microcircuits at the expense of time, space, and energy. Due to the need of a circuit's security, additional lightweight modules are utilised to conceal the circuits while preserving their efficiency.

In this research, we present an encryption logic for safeguarding an ALU while maintaining its operational validity. Due to the fact that insecure systems are susceptible to data leakage and functionality loss, these features are crucial for modern cryptosystems. SECURED PROPOSAL ALU with n bits

The ALU performs arithmetic and logical operations on the inputs (A,B,Cin). The mux assigns any of the computed values to the output based on the selection value (S1S0) specified in Table 1. (result). Each adder and subtractor is composed of n whole adders. The components of a complete

S_1	$S0$	Function
0	0	Addition
0	1	Subtraction
1	0	Comparison
1	1	Multiplication

adder are two half adders and an OR gate. The Comparator was developed using behavioural modelling. MUL consists of the required quantity of AND gates, full adders, and half adders.

TABLE 1: ALU FUNCTION

Fig2: System Overview

Logic for encryption

Through structural modelling, an n-bit ALU is designed, hence enhancing the circuit's flexibility and reusability and expanding its use. Encryption of the generalised n-bit ALU is accomplished by adding encryption logic into a module with extra connections and a bearing on the next level circuit, which influences the majority of the outputs. Consequently, it is easier to determine which node contributed the most to the outcome. These nodes, known as crucial nodes, feature key gates. All ALU submodules, except the comparator, share a complete adder. As a result, the adder fully represents the ALU's encryption. An adder constructed using QCA consists of two half-adders and one OR gate. The outputs of the half adder are sum and carry. As shown in Figure

C_1	K_1	O_2
0	0	C
0	1	$\bar{C}$
1	0	C
1	1	$\bar{C}$

3, we will encrypt the first half of the adder's sum and carry using two key gates, KG1 and KG2. The encryption logic for KG1 and KG2 is

detailed in Tables 2 and 3, respectively.

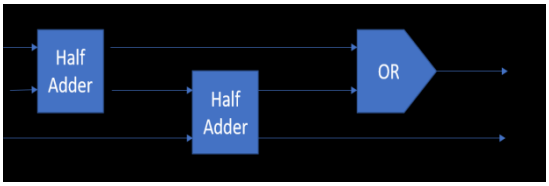


Fig3: Full Adder

Fig 4: Half adder using QCA majority gates

TABLE 2 ENCRYPTION LOGIC FOR KG1

TABLE3 ENCRYPTION LOGIC FOR KG2

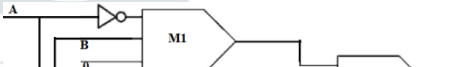
Due to the fact that each ALU submodule has a full adder, no inputs may fail to encrypt for any selection lines (S1S0). Consequently, the supplied key affects the outcomes. This logic is meant to return the appropriate value only when a key is provided. Another benefit is that the opponent is unable of understanding the explanation. An attacker may be ignorant of the CUT's critical and essential inputs. This will prevent the stealing of reasoning.

VEDIC MULTIPLIER

A binary MUL is an electrical circuit used to calculate the product of two binary values in digital devices such as computers. The multiplicand is multiplied using the binary MUL's carbon copy of the traditional multiplication algorithm, with the least significant bit of the MUL coming first. Using two half-adder (HA) modules, a two-bit binary MUL may be constructed. Various computer arithmetic operations can be utilised to implement a digital MUL. Numerous of these techniques involve the computation of a number of partial products that are subsequently combined. Figure 1 depicts a binary 2x2 multiply.

Fig5. 2x2 Binary Multiplier

Vedic MUL operates on Vedic mathematics. If this strategy is used, the system will expand while using fewer hardware components. The Urdhva Tiryakbhyam sutra is utilised by Vedic MUL, which means vertically and horizontally. Figure 6 depicts the block architecture of a 32 bit Vedic multiplier circuit. From the two input bits, two identical chunks are generated. As seen in Figure 6, the vertical and cross products may be calculated using the inputs A[31:0] and B[31:0]. As seen in Figure 6, the two adders are utilised in the design of addition's intermediate stages. The output of these two adders carries Cout and is sent to another RCA. If the bits are not equalised,



S_1	K_0	O_1
0	0	$\bar{S}$
0	1	S
1	0	$\bar{S}$
1	1	S

they should be concatenated. Figure 6 illustrates a 32-bit Vedic multiplier.

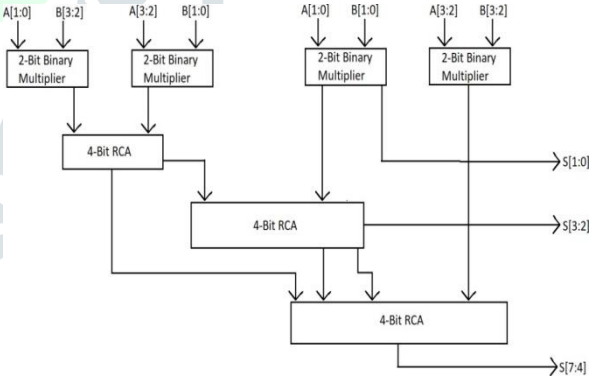


Fig6:4-Bit Vedic MUL.

Ripple Carry Adder(RCA) ADDER

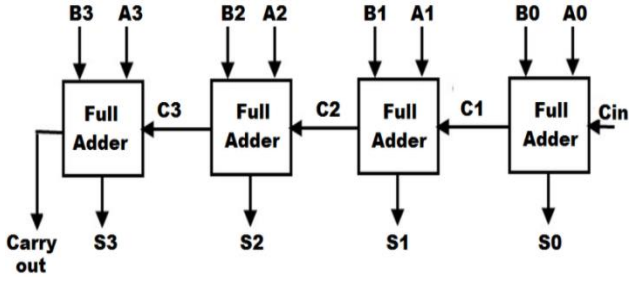


Fig8: 4-bit Ripple Carry Adder

COMPARATOR

A magnitude digital Comparator is a

combinational circuit that compares two digital or binary values to determine whether one is more than, equal to, or less than the other. Using two A and B inputs and three output terminals—one for the A > B condition, one for the A = B condition, and one for the A< B condition—we construct a logical circuit.

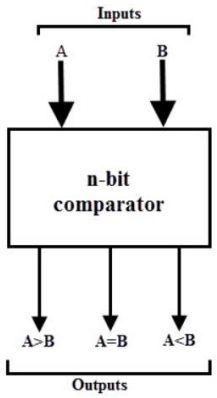


Fig9: Block Diagram of nbit Comparator

SUBTRACTOR

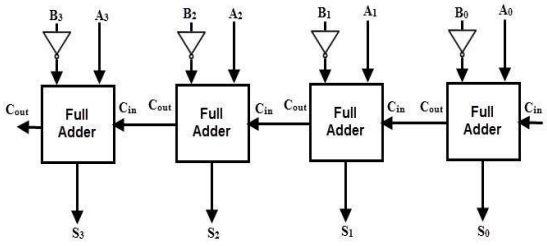
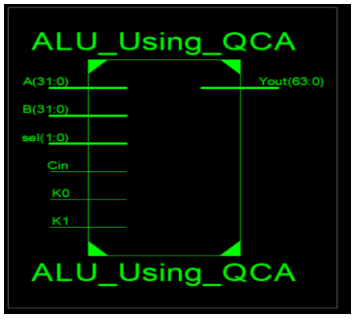


Fig10: 4 Bit Subtractor Using 2's Complement

4.RESULTS

RTL SCHEMATICRTL is a blueprint for an architectural design that is utilised to verify whether or not it conforms to our ideal design. Using Verilog or VHDL, a description of the architecture must be transformed into a functional summary. The RTL architecture includes internal connection blocks to simplify debugging. The graphic below depicts the RTL



schematic for the intended architecture.

Figure 11: Proposed ALU RTL Schematic

TECHNOLOGY SCHEMATIC: When utilising the technology diagram, the architecture is represented by a LUT area parameter. The FPGA LUTs indicate how memory was allocated by the programme.

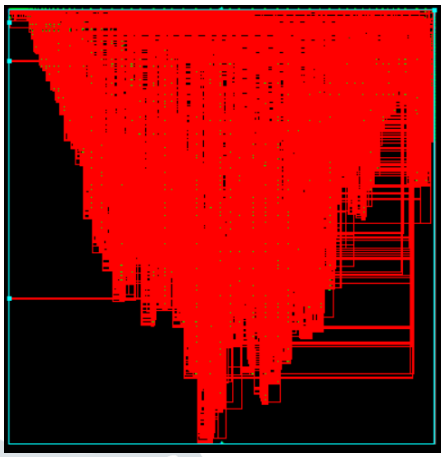


Fig12:View Technology Schematic of proposed ALU

SIMULATION: The simulation approach is referred to be a final verification in terms of its operation, whereas a schematic is a verification of the connections and blocks. When the tool's home screen is switched to the simulation screen, only wave forms may be generated. In this instance, it may offer a variety of radix number systems.

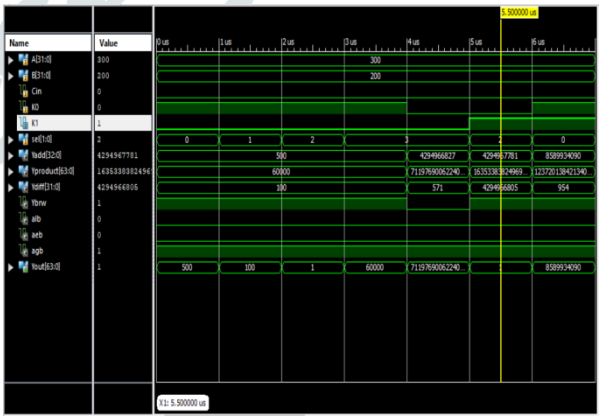


Fig13: Simulated Waveforms of proposed ALU

PARAMETERS: In the case of VLSI, important considerations are size, latency, and power. XILINX 14.7 written in verilog is utilised to extract the delay parameter.

Device utilization analysis

The investigation utilised the xc3s500e device from the Spartan 3E family's fg320 package. As seen in Table, despite its encryption and reusability, our created ALU needs much fewer device resources than a typical 32 bit ALU. The 32-bit ALU of this project is both efficient and secure. The gadget utilisation data verifies and supports our aim of achieving optimum efficiency. The key is input precisely only if an efficient and encrypted ALU is constructed, which only yields accurate results.

Parameter	Existed ALU	Proposed ALU
No of LUTs	5086	4906
Power (Watt)	44.240	42.674

Table4: Parameter Comparison Table.

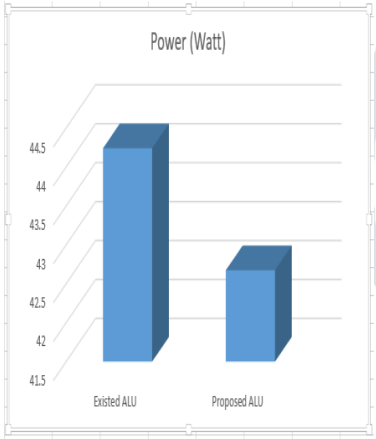


Fig15 : Power Comparison Bar Graph.

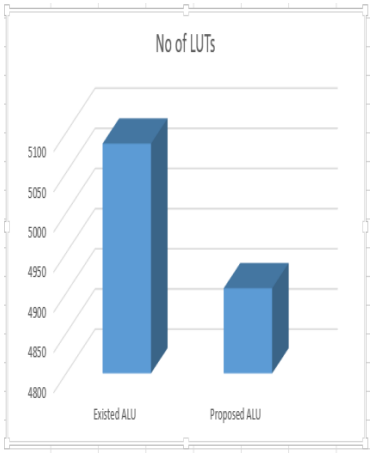


Fig 16: LUTs Comparision Bar Graph

CONCLUSION

The structurally modelled n-bit ALU was derived from the behaviorally modelled 32-bit ALU, hence increasing its flexibility and reusability. Individual modules were constructed using QCA majority gates. QCA on the Nano scale has a brighter future than analogous implementations based on classical Logic Gates because to its improved performance in terms of clock frequency, device density, and power consumption. To protect the ALU and give a better level of security, the basic sub-circuit module provides a common encryption logic for all higher-level modules that have a greater effect on the output. The encrypted ALU is provided with two-bit keys and its outputs are validated against all four key combinations (K1K0). The selection line inputs (S1S0) govern the functioning of the ALU, while the key inputs affect the precision of the output (K1K0). The only key that produces the proper answer is "K1K0 = 01." For improper key combinations, the output deviates greatly from the anticipated output, resulting in a false positive that confuses the opponent.

REFERENCES

[1] S. Akhter, "VHDL implementation of fast NxN MUL based on Vedic mathematics," in Proc. 18th European Conference on Circuit Theory and Design, 2007, pp. 472-475

[2] S. Nagaraj, Dr.G.M. Sreerama Reddy and Dr.S. Aruna Mastani; A Comparative Study on Different MULs-SurveyJournal of Advanced Research in Dynamical and Control Systems14739-7522018Institute of Advanced Scientific Research.

[3] M.Pushpa, S. Nagaraj, Design and Analysis of 8-bit Array, Carry Save Array, Braun,Wallace Tree and Vedic MULs, IEEE Sponsored International Conference On New Trends In Engineering & Technology(ICNTET 2018).

[4] Nagaraj, S; Thyagarajan, K; Srihari, D; Gopi, K; Design and Analysis of Wallace Tree MUL for CMOS and CPL Logic2018 International Conference on Computation of Power, Energy, Information and Com-

munication (ICCPEIC)006-0102018IEEE

[5] Josmin Thomas ; R. Pushpangadan ; S Jinesh Comparative study of performance Vedic MUL on the Basis of Adders used 2015 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE)

[6] S. Nagaraj, Dr.G.M. Sreerama Reddy and Dr.S. Aruna Mastani; A Survey on Adiabatic LogicInternational Conference on Communications, Signal Processing and VLSI(IC2SV2019),Springer Conference ,National Institute of Technology, Warangal.

[7] S. Nagaraj,K.Venkataramana Reddy and and P.Anil Kumar3i;Analysis of Vedic MUL for Conventional CMOS & Complementary Pass Transistor Logic(CPL) Logics SCOPUS Indexed Springer 8th Interna- tional Conference on Innovations in Electronics and Communication Engineering, (ICIECE-2019)
.

[8] Au L.S. and Burgess N. (2002), "A (4:2) adder for unified GF(p) and GF(2n) Galois field MULs", Proceedings of 36th IEEE Asilomar Conference on Signals, Systems, and Computers, vol. 2, pp. 1619-1623.

[9] Chittibabu A., Sola V.K. and Raj C.P. (2006), "ASIC Implementation of New Architecture for constant coefficient Dadda MUL for High-Speed DSP applications", Proceedings of the National Conference on Recent trends in Electrical, Electronics and Computer Engineering, JCECON, pp. 299 – 304.

[10] Ramesh Pushpangadana, Vineeth Sukumarana, Rino Innocenta, Dinesh Sasikumara & Vaisak Sundara,"High Speed Vedic MUL for Digital Signal Processors",IETE JOURNAL OF RESEARCH , Vol 55, ISSUE 6 , NOV-DEC 2009.