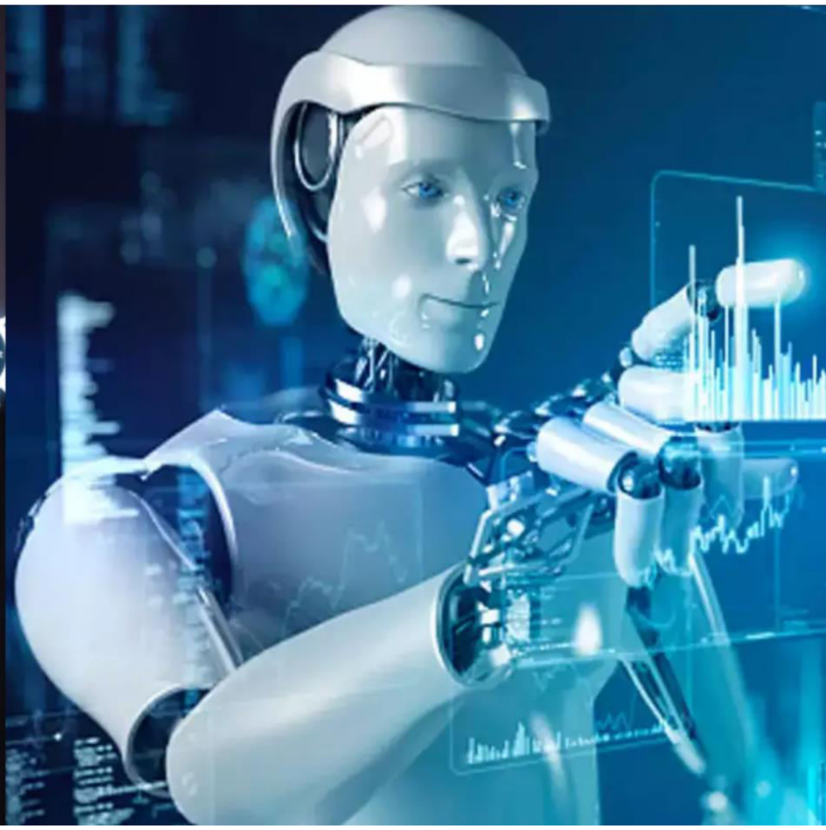
IJIRSET
International Journal of Innovative Research in
Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 6, June 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406040|

Design and Implementation of 16 Bit ALU for Enhanced Security using Key Gate Concept

P Santhosh

Associate Professor, Department of Electronics & Communication Engineering, Hyderabad Institute of Technology and Management, Hyderabad, India

G Tisha, J Shivani, M Ashrutha, R Jagan Mouli

B.Tech. Final Year, Department of Electronics & Communication Engineering, Hyderabad Institute of Technology and Management, Hyderabad, India

ABSTRACT: In modern digital systems, the Arithmetic Logic Unit (ALU) is integral to processing, serving as the computational core of every Central Processing Unit (CPU). As the demand for secure and adaptable hardware intensifies, this project introduces a 16-bit ALU designed using Verilog with an emphasis on enhanced security. By integrating key-based control logic, the ALU ensures functional correctness only when a predefined key combination is provided, thereby safeguarding against unauthorized access and potential hardware threats. The proposed architecture is structurally modeled to support flexibility and reusability across multiple applications without compromising performance. This approach contributes a reliable solution to mitigate vulnerabilities such as hardware Trojans and IP theft in sensitive digital environments. Potential application domains include embedded systems, IOT, cryptographic modules, and secure signal processing unit.

KEYWORDS: **Arithmetic Logic Unit (ALU)**
The core of the design performs 16-bit arithmetic and logic operations, such as addition, subtraction, AND, OR, XOR, and more. It is structured in Verilog to provide modularity and ease of reuse, supporting rapid integration into larger digital systems.

Key Gate Security Mechanism
This is the security-enhancing feature of the design. It uses a key input (K1K0) to control the operational integrity of the ALU. The correct functionality is guaranteed only when the correct key (K1K0 = 10) is applied. Any incorrect key leads to faulty output, making reverse engineering or unauthorized usage ineffective.

I. INTRODUCTION

In today's digital era, the Arithmetic Logic Unit (ALU) serves as the core computational component within the Central Processing Unit (CPU) of nearly every digital system. It performs fundamental operations such as arithmetic calculations and logical processing, which are essential to system performance. As technology advances and the complexity of hardware grows, ensuring the functional integrity and security of the ALU has become a critical design consideration.

Conventional ALU designs often focus on speed, efficiency, and area optimization. However, with the rising threat of hardware-level attacks such as reverse engineering, IP theft, and hardware Trojans, there is a growing need for secure hardware architectures. To address this concern, this project proposes the design and implementation of a 16-bit

ALU that integrates a security mechanism based on a key gate concept.

The proposed ALU is implemented using Verilog and operates correctly only when a specific key input is provided. Incorrect keys trigger erroneous outputs, thereby preventing unauthorized access and enhancing resistance to malicious exploitation. This key-dependent design introduces a layer of logical obfuscation without compromising the performance of the ALU.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406040|

By combining structural modeling in Verilog with a key- based security approach, this project aims to contribute a flexible, reusable, and secure ALU design suitable for embedded systems, IoT applications, and hardware cryptography environments.
Used for synthesizing the design, verifying its functionality, and implementing it on FPGA hardware. This toolchain provided a complete environment for designing, testing, and analyzing the performance and security of the proposed ALU architecture.It enables programming of the bot's navigation, sensor management, and actuator control, ensuring efficient and real-time operation shown in fig 1

II. MOTIVATION

The ALU is a critical component of any CPU, responsible for performing arithmetic and logical operations. With the growing use of digital systems in security-sensitive applications like embedded systems and IoT, hardware-level security has become essential. Traditional ALUs prioritize performance but often lack protection against threats such as reverse engineering and hardware Trojans.

This project is motivated by the need to design a secure 16-bit ALU that maintains functionality while preventing unauthorized access. By introducing a key gate mechanism, the ALU produces correct results only when a valid key is supplied, enhancing its resistance to tampering and misuse.

III. RELATED WORK

The logic obfuscation using key gates to enhance hardware security and protect against reverse engineering and IP theft. Chakraborty and Bhunia demonstrated that inserting key gates can secure circuits but introduces power and area overheads. Richards emphasized structural-level design for reusability and scalability, while Chandini et al. proposed functional obfuscation to further complicate reverse engineering. These works collectively highlight the trade-off between security and design efficiency, motivating our secure 16-bit ALU design using embedded key-gate encryption.

IV. SOFTWARE USED

A. XILINX VIVADO

The software tools utilized in this project include Xilinx Vivado Design Suite and Verilog HDL. Verilog was employed to model and simulate the 16-bit ALU using both structural and behavioral approaches. Xilinx Vivado was then

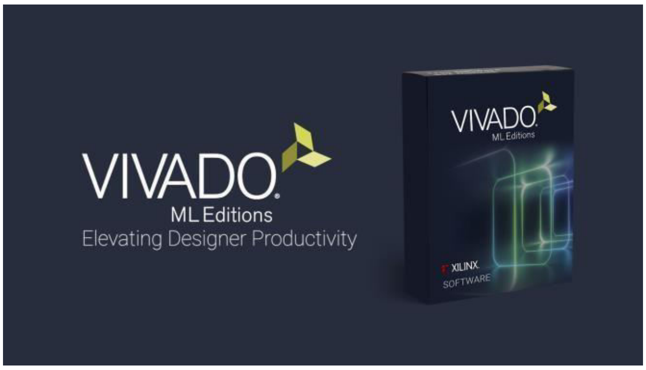


Fig. 1. XILINX VIVADO

B. VHDL

VHDL (VHSIC Hardware Description Language) is a hardware description language used to model and design digital systems, particularly for FPGAs and ASICs. In the context of the Eco Mender Bot project, VHDL would be used to describe the bot's FPGA-based logic, enabling control over its sensors, actuators, and communication systems. The language allows developers to define how the bot should process data from its environment, navigate autonomously, and interact with the Eco Center in real-time. By writing VHDL code, the team can implement efficient, parallel

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406040|

processing logic that enhances the bot's performance in terms of speed, accuracy, and energy efficiency. VHDL is crucial for creating the custom hardware architectures that will drive the Eco Mender Bot's behavior and decision-making processes.

V. PROPOSED MODEL

The proposed model is a 16-bit Arithmetic Logic Unit (ALU) embedded with encryption logic using key gates to enhance hardware-level security. This model performs standard arithmetic and logical operations—such as addition, subtraction, comparison, and shifting—while integrating a key-based obfuscation mechanism. The encryption is embedded within critical sub-modules, particularly the full adder, by inserting key gates that ensure correct output only when the right key combination is applied. This approach not only secures the ALU against reverse engineering and hardware Trojans but also maintains its functional integrity and reusability across applications. The model is developed using Verilog HDL and implemented using Xilinx Vivado.

VI. RESULTS AND DISCUSSIONS

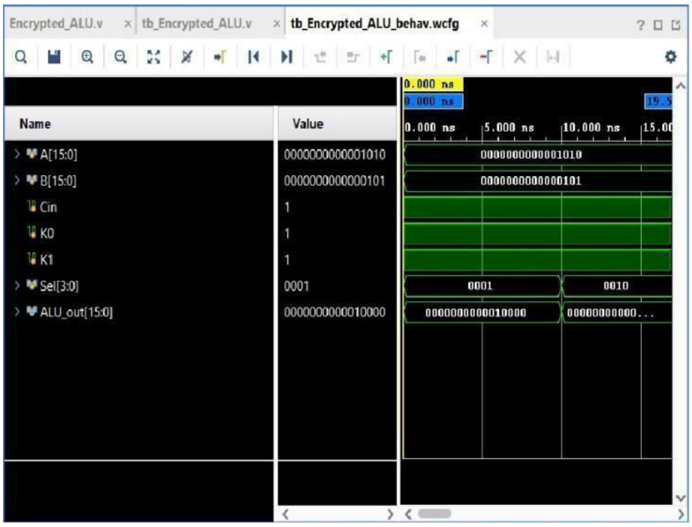


Fig 2. waveforms for 16-bit encrypted ALU

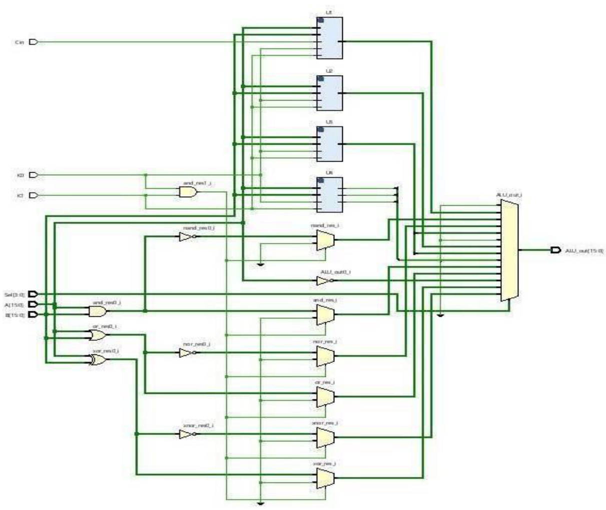


FIG 3. Schematic view of 16-bit ALU

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406040|

VII. CONCLUSION

The project successfully demonstrates the design and implementation of a secure 16-bit ALU using key gate-based logic obfuscation. By embedding encryption logic within critical modules like the full adder, the ALU ensures correct functionality only when the correct key is applied, thereby enhancing protection against reverse engineering and unauthorized access. Developed using Verilog HDL and implemented in Xilinx Vivado, the design maintains efficiency in terms of area, power, and performance while adding a crucial layer of hardware security. This approach provides a scalable and effective solution for secure digital system design.

REFERENCES

1. S. Nagaraj,K.Venkataramana Reddy and and P.Anil Kumar3i;Analysis of Vedic Multiplier 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)
2. 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.
3. Govindaraj, V; Nagaraj, S; Kumar, J Madan; Test Pattern Generator for Low Power Bist
4. Applications Journal of Advance Research in Dynamical and Control Systems ISSN 1943- 023x10Social Issue 12-Special Issue659-6642018
5. M.Pushpa, S. Nagaraj, Design and Analysis of 8- bit Array, Carry Save Array, Braun,Wallace Tree and Vedic Multipliers, IEEE Sponsored International Conference On New Trends In Engineering & Technology(ICNTET 2018).
6. S.Nagaraj, Dr.G.M. Sreerama Reddy and Dr.S. Aruna Mastani; A Comparative Study on Different Multipliers-SurveyJournal of Advanced Research in Dynamical and Control Systems14739- 7522018Institute of Advanced Scientific Research.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE
SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details