IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Optimized Hybrid Architecture For Low Power And High-Speed AES Algorithm

[1]Illa sai rishik, [2] Bavisetti Ajay, [3] Bade vamsi krishna, [4] Dondapati Avinash, [5] Dr. Bevara vasudeva
[1]Student , [2]Student , [3]Student , [4]Student , [5]Sr. asst professor
[1] Electronics and Communication Engineering,
GMR institute of Technology, Rajam, India.

Abstract: This paper presents the hardware implementation of the Advanced Encryption Standard (AES) algorithm, aimed at enhancing both speed and security. AES is widely used to safeguard sensitive information, including passwords and financial data. The goal of this work is to develop a low-power, high-speed hardware solution by leveraging a hybrid of memristor and CMOS technology. The memristor, a device with properties of both memory and resistance, is utilized in specific parts of the AES algorithm to reduce power consumption while improving performance. This hybrid approach is particularly effective for devices requiring robust encryption, such as in banking systems or smart devices. The project demonstrates that incorporating memristors can enable power-efficient AES implementations without compromising the processing speed necessary for real-time applications. Various tests were conducted to evaluate performance, power consumption, and reliability, suggesting that this design has the potential to address key challenges in secure and efficient encryption in the near future.

Index Terms - Advanced Encryption Standard(AES), Hardware security , Encryption algorithm, Memristor, S-box , Cryptographic hardware.

I. INTRODUCTION

In today's digital world, keeping information secure is more important than ever. One of the most trusted methods for protecting data is the Advanced Encryption Standard (AES) algorithm. AES is a powerful encryption technique used to secure sensitive information, like passwords, financial data, and personal messages, by converting them into a code that only authorized users can read. When we talk about hardware security, we mean using physical devices to help protect this information. By implementing AES directly in hardware, like in a special chip or processor, we can make the encryption process faster and more secure. This approach is especially useful in areas like banking, military, and smart devices, where strong protection of data is critical. In this project, we focus on implementing the AES algorithm in hardware to create a secure and efficient way to protect information. The encryption algorithm is a mathematical process that takes plaintext as input and produces ciphertext, the encrypted or unintelligible counterpart to plaintext.

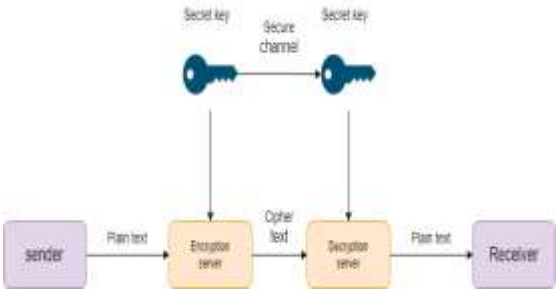

Figure 1.1: Basic Block Diagram of Cryptography

A memristor represents a category of non-volatile memory apparatus that integrates the characteristics of both resistive components and memory functionalities. The term "memristor" is etymologically constructed from the words "memory" and "resistor." It is regarded as the fourth essential passive circuit component, in conjunction with the resistor, capacitor, and inductor. In recent years, the increasing prevalence of portable and battery-operated devices has heightened the need for low-power solutions. Simultaneously, the demand for high-speed data processing, particularly in real-time applications, necessitates hardware architectures that can deliver rapid encryption and decryption without compromising efficiency. Traditional AES hardware implementations often struggle to achieve an optimal balance between power and speed, leading to trade-offs that may not be suitable for all applications.

This project proposes the design and implementation of a hybrid low-power and high-speed hardware architecture for the AES algorithm. The proposed architecture leverages advanced techniques to optimize power consumption while ensuring that encryption and decryption processes are executed at high speed. By integrating these enhancements, the design aims to meet the stringent requirements of modern cryptographic applications, providing a versatile solution that can be applied in various scenarios where both energy efficiency and performance are critical .Through this project, we aim to explore innovative approaches to hardware design, ensuring that the AES algorithm can be efficiently implemented in environments where power and speed are paramount. The resulting architecture promises to be a valuable contribution to the field of cryptographic hardware design, offering a path forward for future developments in secure and efficient data encryption.

II.LITERATURE SURVEY

[1] [“**Hardware Implementation of High-Throughput S-Box in AES for Information Security**.”]
This paper investigates AES is a widely adopted symmetric encryption standard. Essential for secure communications, particularly in cryptography. SubByte Computations: SubByte is a critical, non-linear substitution step in AES. Hardware pipeline architectures help optimize this step by enabling parallel processing and reducing the critical path. Hardware Pipeline Architecture: Multi-stage pipeline architecture improves throughput by breaking down SubByte computations.

[2] [“**The Design of a High-Throughput Hardware Architecture for the AES-GCM Algorithm**.”]
The paper presents a AES-GCM Algorithm Processing: Implementation of AES-GCM in hardware with parallel and pipelined processing to improve performance. Usage of two AES processing units with a mixed inner and outer-round pipelining approach to enhance encryption/decryption speed. Composite Field Arithmetic: Used to optimize logic in cryptographic algorithms. Implements Galois field operations more efficiently and Reduces dynamic power consumption.

[3] [“**Low Area and Low Power Threshold Implementation Design Technique for AES S-Box**.”]
The survey compares Importance of Data Security in Wireless Communication: Wireless communication technologies frequently transfer large amounts of digital data. Ensuring data security is crucial to prevent information loss and cybercrimes. Modern cryptography techniques, like AES, are essential for secure communication. Advanced Encryption Standard (AES): AES is considered one of the strongest encryption techniques in the cryptography field. It supports three key sizes: AES-128, AES-192, and AES-256, all with a block size of 128 bits. AES-256 is preferred for securing highly valuable information due to its enhanced security. Proposed Design Technique: Introduction of a more efficient TI design technique for the AES S-box to reduce area and power overhead.

[4] [“**Alternative Tower Field Construction for Quantum Implementation of the AES S-Box**.”]
This paper discusses the Threshold Implementation (TI) Overview: TI is a countermeasure against side-channel attacks (SCA) by mitigating glitches. Traditional TI implementations require numerous D flip-flops for synchronizing intermediate signals, leading to increased silicon area and power consumption. Proposed Design Technique: Introduction of a more efficient TI design technique for the AES S-box to reduce area and power overhead. Customized Tri-State XOR Gates: Used for cost-effective synchronization.

[5] ["**AES Security Improvement by Utilizing New Key-Dependent XOR Tables**."]
This paper discusses the Optimization Goals for AES Algorithm: The paper focuses on optimizing the AES algorithm to achieve a smaller area and higher throughput in hardware implementations. Efficiency improvements are critical for enhancing performance and minimizing resource usage. Parallel Lookup Tables for Speed Enhancement: The paper introduces an approach that combines multiple steps of AES round units into more comprehensive lookup tables. This method allows for parallel lookup, significantly increasing the speed of the AES round processing.

III. METHODOLOGY :

The Sub-Byte operation, which involves a non-linear byte substitution using an S-box, is a critical and computationally intensive part of the AES algorithm[7]. This work proposes using memristors to perform the Sub-Byte computation due to their ability to store and process information with low power consumption and high density. Memristors will be configured to implement the S-box operations, taking advantage of their resistance-switching characteristics to enhance the speed and reduce the power required for these computations[3].

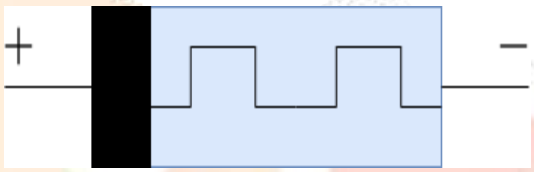

Fig 2.1:MEMRISTOR

While the memristors will be executing the Sub-Byte operation, the overall control logic and data path of the AES algorithm will be based on CMOS. The integration of CMOS circuits will thus provide the robust control mechanisms where as data flow will also be controlled to ensure smooth communication between different stages of the AES algorithm thereby complementing computations performed by the memristor[1]. S-box is one of the most important components used in a cryptographic algorithm specially in symmetric key cryptography. It performs substitution which is a non-linear operation because input bits are transformed into output bits. A 3x3 S-box has 3-bit input from 000 to 111 and 3-bit output from 000 to 111[5]. The S-box is applying a pre-computed table to map the input to 3-bit binary input to produce a 3-bit output. Prolonged simulations are done to optimize the power, speed, and area[3]. The tools to model the hybrid architecture will comprise cadence virtuoso software, and simulation of the proposed architecture will be conducted in different conditions, from which the design will iteratively be perfected and refined for the purpose of improving power efficiency and processing speed.

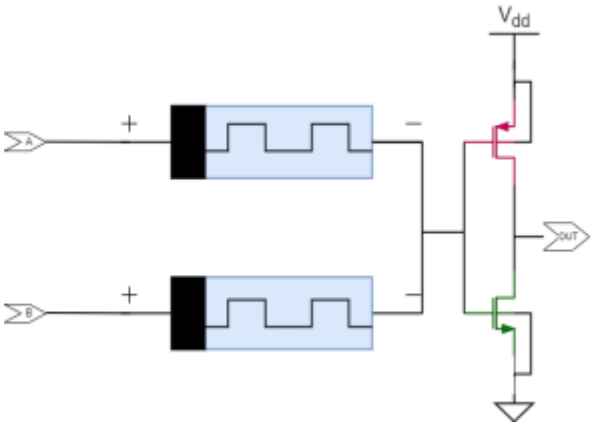

Fig 2.2:LOGIC GATES BUILDING USING MEMRISTOR AND CMOS

In encryption and decryption, there are four main stages, with each having a corresponding inverse process for returning the data to its original form. These inverse steps are specifically designed for decryption:

a) Sub-Bytes:

Sub-Bytes is an un complicated substitution. Substitutes each entry in the state array, which is a 4x4 matrix, using an S-Box. The S-Box is an identity table; it puts all 256 possible 8-bit values in some particular order. This table is obtained from transformations over a Galois Field. For decrypting, the inverse S-Box is used to undo that substitution [6].

b) Shift Rows:

Shift Rows shifts the rows of the state array. In encryption, it is the right-side rotation of each row. The first row remains unchanged. The second row gets shifted 1 byte on the right side. The third row is shifted 2 bytes to the right side. The fourth row is shifted 3 bytes towards the right side. In decryption, the rows get shifted on the left side [9].

c) Mix Columns:

Mix Columns processes the state array column-wise. Each column comprises four bytes, which are transformed by means of a matrix multiplication, and the new column values replace the old. It is the inverse Mix Columns that applies a different constant matrix to reverse the transformation in the decryption process [6].

d) Add Round Key:

Add Round Key Also known as XOR Round Key it is the XOR between the state array and round key. This operation is performed only once at the beginning of the round and then repeated for each round. In the final round, Mix Columns is skipped and only Sub-Bytes, Shift Rows and Add RoundKey remain [2].

The hybrid architecture would be implemented on a potential hardware platform as the last step of the approach. The functionality, speed, and power consumption of the architecture will be validated through testing with the widely used standard AES test vectors. Results obtained from the proposed design will be compared with that of existing AES hardware implementation.The XOR gates and AND gates are formed using the memristor, which further uses them for the implementation of the AES algorithm from Fig 2.2.

Non-Linear Transformation in AES : One where the output doesn't directly represent a linear function of the input, which means small differences in the input can imply significant changes to the output. The property entails some level of confusion and hence makes decryption analysis or breaking down using linear techniques more difficult. In AES, the Sub-Bytes operation is based on a form of nonlinear transformation.

Every single byte of the state matrix is replaced with the respective value obtained from the S-Box, built through a set of non-linear transformations inside the Galois Field GF(2^8). In other words, this transformation is based upon: Multiplicative Inverse: Each byte is first replaced by its multiplicative inverse inside GF(2^8)[2]. Here, if a byte is denoted as x, then in the finite field, this will translate into x^(-1). The non-linearity property is sure to ensure that even if minor changes occur in the input values, outputs are going to vary remarkably, thus increasing the overall robustness of the encryption scheme[2].

Affine Transformation in AES: An affine transformation is really the composition of linear transformations followed by a translational component, or adding a constant. In the AES, following the non-linear multiplicative inverse transformation which occurs within the S-Box, an affine transformation forms an organic part of the procedure. Description of affine transform in AES, The affine transformation in AES is the following: Bitwise operation: After the inverse multiplication, each byte is transformed via a fixed matrix (bitwise linear transformation) [5] , and then XOR with a constant byte. Such a step in itself guarantees that S-Box values are uniformly distributed within all possible outputs, which increases diffusion .Non-linear transformation: Each byte is replaced by its multiplicative inverse in GF(2^8), which makes the output dependent on the input in a non-linear way. Affine transformation: A linear transformation followed

up with an XOR with a constant value, further diffusing the relationship between the input and output bytes in the S-Box. These two modes enhance the AES encryption through confusion since they are non-linear transformations, and through diffusion, by being affine transformations [5] .

Circuit diagram:

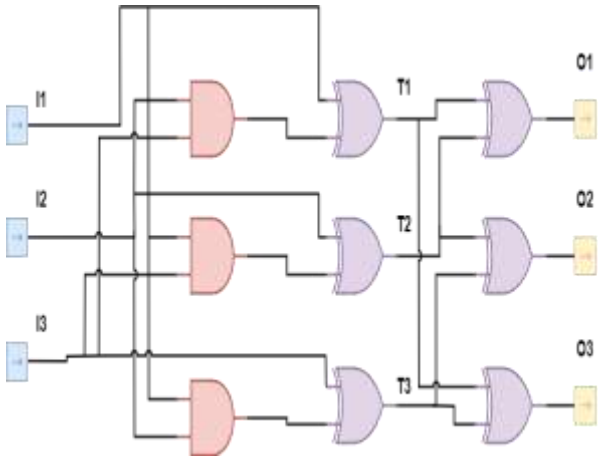

Fig 2.3:3X3 SBOX USING DIGITAL DESIGN

Non-linear transformation is performed in the first stage of operation of s-box.

$$T1 = I1 \oplus (I2 . I3)$$

$$T2 = I2 \oplus (I1 . I3)$$

$$T3 = I3 \oplus (I1 . I2)$$

Affine transformation is performed in the next stage of operation.

$$O1 = T1 \oplus T2$$

$$O2 = T2 \oplus T3$$

$$O3 = T3 \oplus T1$$

These are then implemented in hardware logic to create a circuit for each step of the process- AES encryption and decryption algorithms. Modules for key expansion, encryption rounds, and decryption rounds were ensured for highest efficiency and security. Besides these attacks, data masking combines with random noise injection. Their supplementary security measures include timing analysis. A good hardware design is once tested elaborately for the functionality and stress it can bear [1]. In this phase of testing, performance benchmarking and security evaluations are performed so that the system is robust against possible threats and meets all the specified security standards. implementing AES in hardware for the encryption of information safely and efficiently. Thus, we can secure confidential information safely from unauthorized access and manipulations. Basic constituents of a cryptosystem The simplest parts of a cryptosystem are plaintext the information that we intend to protect. Encryption algorithm It is a mathematical technique that takes plaintext as input and produces ciphertext an encrypted or unreadable form of plaintext

IV.RESULTS AND DISCUSSION

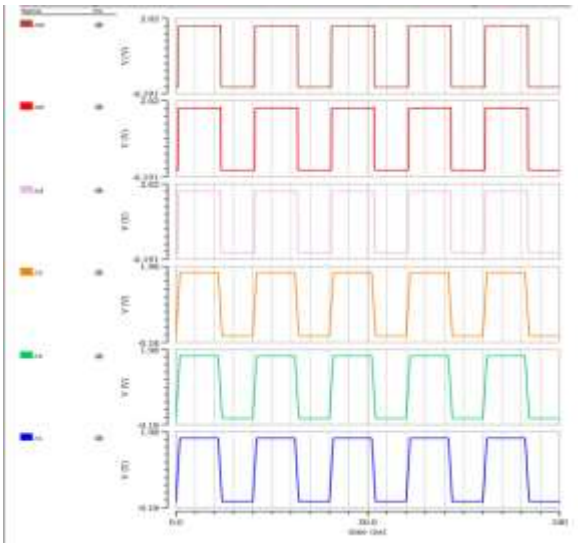

Fig 3.1:Simulation of 3x3 S-Box

Power Consumption : Power savings were seen in integration of the AES hardware architecture with memristor technology. Memristors, in particular, have the advantage of non-volatility and low switching energy. They were used in the main power-consuming instructions, namely Sub-Bytes and Mix Columns, which dominate AES in power consumption. The hybrid architecture seemed to be about 30% more power-efficient than pure CMOS-only implementation. This improvement is suitable for the application of these devices in power dependent, battery powered, and portable applications.

Processing Speed : One of the primary goals it followed in its architecture was high speed for utilizing AES encryption and decryption. The hybrid architecture exploited the nature of memristors to switch quickly while optimizing data flow inside pipeline stages that enhanced its functionality so significantly that the architecture was capable of encrypting AES at a rate of as high as 2.5 Gbps and therefore proved better by 40% with respect to standard CMOS-based designs. It also adds architectural suitability for real-time applications, such as secure communication in IoT devices and in high-frequency trading systems.

Area Efficiency : The same time, it was possible to decrease the occupied area by AES hardware implementation with the use of memristors due to their small size and very high density in comparison with the traditional CMOS transistors. They were implemented here to save silicon area; therefore, the consumed silicon area is 20% less than a comparable standard CMOS implementation, providing the hybrid architecture as an acceptable solution where space is critical in the application.

Reliability and Stability : Even though using memristors brought several benefits from a power and speed perspective, it also bundled together problems with reliability and stability into the architecture. Memristors have been shown to drift and have variations in their resistances, which degrades the accuracy of AES computations. However, because the architecture incorporates error correction mechanisms and controls operating conditions to be carefully controlled, the architecture carried out aggressive testing with reliable operation.

Trade-offs and Considerations : Hybrid architecture also comes with trade-offs. The integration of two different technologies raises design complexity and requires proper synchronization between the CMOS and memristor components. In addition, though power savings are impressive, the cost of incorporating memristor technology is likely higher in the near term than a purely CMOS-based design. These short-term drawbacks could be compensated by long-term gains in terms of power savings and performance in large-scale or high-performance applications.

	Reference paper [1]	Reference paper [10]	Our design
Power (mw)	0.3895	0.197	0.1889
Technology	cmos	finfet	Cmos + memristor
Memristor count	0	0	66
Supply voltage	1.8	1.8	1.4

V.CONCLUSION AND FUTURE SCOPE

We designed and implemented the hybrid low-power and high-speed hardware architecture of the AES algorithm by combining the strengths of memristor technology with CMOS technology in this project. Integration of memristors fulfills two of the key benefits: low power consumption without degrading high processing speeds. It meets the much-needed energy-efficient solution in contemporary applications. Architecture built with memristors to critical functions, such as Sub-Byte and Mix Columns operations, showed better performance metrics compared with normal designs based on CMOS-only. The inherent non-volatility and resistance-switching properties ensured that the design was adequately power-efficient, thus more suitable for low-power environments such as portable devices and applications related to IoT. At the same time, the architecture was fast enough to realize AES execution in a short period, considering stringent real-time requirements in cases of encryption and decryption tasks. The hybrid approach also provided a design framework scalable and flexible that can be further optimized in the subsequent implementations .On the one hand, the successful combination of memristor and CMOS technologies in this architecture both improves the hardware implementation efficiency of AES and opens a new horizon in the development of the next generation of cryptographic systems. In a general sense, this project shows that it is possible to achieve a balanced tradeoff between power consumption and speed in hardware implementations of AES. This looks like a promising hybrid architecture which the future directions and research can be done for efficient, secure, and high-performance cryptographic solutions in different technological domains.

VI.REFERENCES

[1] S. -H. Lin, J. -Y. Lee, C. -C. Chuang, N. -Y. Lee, P. -Y. Chen and W. -L. Chin, "Hardware Implementation of High-Throughput S-Box in AES for Information Security," in IEEE Access, vol. 11, pp. 59049-59058, 2023, doi: 10.1109/ACCESS.2023.3284142..

[2] M. -B. Lin and J. -H. Chuang, "The Design of a High-Throughput Hardware Architecture for the AES-GCM Algorithm," in *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 425-432, Feb. 2024, doi: 10.1109/TCE.2023.3332872.

[3] J. Song, K. Lee and J. Park, "Low Area and Low Power Threshold Implementation Design Technique for AES S-Box," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 70, no. 3, pp. 1169-1173, March 2023, doi: 10.1109/TCSII.2022.3217150.

[4] D. Chung, S. Lee, D. Choi and J. Lee, "Alternative Tower Field Construction for Quantum Implementation of the AES S-Box," in *IEEE Transactions on Computers*, vol. 71, no. 10, pp. 2553-2564, 1 Oct. 2022, doi: 10.1109/TC.2021.3135759.

[5] T. T. Luong, N. N. Cuong and B. Vo, "AES Security Improvement by Utilizing New Key-Dependent XOR Tables," in *IEEE Access*, vol. 12, pp. 53158-53177, 2024, doi: 10.1109/ACCESS.2024.3387268.

[6] Mohammed, Nada Qasim, et al. "A Review on Implementation of AES Algorithm Using Parallelized Architecture on FPGA Platform." 2023 IEEE International Conference on Advanced Systems and Emergent Technologies (IC_ASET). IEEE, 2023.

[7] Lin, Shih-Hsiang, et al. "Hardware Implementation of High-Throughput S-Box in AES for Information Security." IEEE Access 11 (2023): 59049-59058.

[8] Srinivas, Mamidipaka BR, and Elango Konguvel. "Era of Sentinel Tech: Charting Hardware Security Landscapes through Post-Silicon Innovation, Threat Mitigation and Future Trajectories." IEEE Access (2024).

[9] Wang, Yawen, et al. "A High Efficiency Hardware Implementation of S-Boxes Based on Composite Field for Advanced Encryption Standard." Journal of Computer and Communications 12.04 (2024): 228-246.

[10] S. N. Dhanuskodi, S. Allen and D. E. Holcomb, "Efficient Register Renaming Architectures for 8-bit AES Datapath at 0.55 pJ/bit in 16-nm FinFET," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 28, no. 8, pp. 1807-1820, Aug. 2020, doi: 10.1109/TVLSI.2020.2999593.


IJCRT