International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Low-Power Implementation of Advanced Encryption Standard Using Verilog HDL

1S.Penchala Reddy, Associate Professor,Dept of ECE,PBR VITS,Kavali,Andhra Pradesh,India.
2345,I.Anusha,PG Student, Department of Electronics and Communication Engineering,
PBR Visvodaya Institute of Technology & Science, Kavali (Autonomous), SPSR
Nellore (Dt.), Andhra Pradesh – 524201, India

Abstract - The Advanced Encryption Standard (AES) is a widely used symmetric key encryption algorithm that secures digital data in modern communication systems. Conventional AES hardware implementations often consume high power, limiting their efficiency in resource-constrained environments. This paper presents a low-power AES hardware design implemented in Verilog HDL. The base design uses AES-128 with a 128-bit data block and 128-bit key, while the proposed design enhances security with a 256-bit key. Flip-flop based clock gating is applied to reduce dynamic power by minimizing unnecessary switching activity. Simulation results demonstrate that the proposed architecture effectively reduces power consumption while maintaining encryption performance, making it suitable for applications in IoT devices, embedded systems, and other low-power environments.

Key Words: Advanced Encryption Standard (AES), Verilog HDL, Clock Gating, Low-Power Design, Cryptographic Hardware, Power Optimization, AES-128, AES-256.

1. INTRODUCTION

With the rapid advancement of digital communication systems, ensuring data security has become a major concern. Cryptographic algorithms are widely used to protect sensitive information from unauthorized access and modification. Among these techniques, the Advanced Encryption Standard (AES) is one of the most secure and widely adopted symmetric key encryption algorithms.

AES operates on a 128-bit data block and supports key sizes of 128, 192, and 256 bits. The number of encryption rounds depends on the key size, where AES-128 uses 10 rounds and AES-256 uses 14 rounds. Each round includes SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations, along with a key expansion process that generates round keys. Although, hardware implementations of AES provide high speed and strong security, they often result in increased power consumption due to continuous clock activity. This becomes a major limitation in low-power and embedded systems where energy efficiency is critical. To address this issue, power optimization techniques such as clock gating are used to reduce unnecessary switching activity.

In this work, an improved AES architecture is proposed by upgrading from AES-128 to AES-256 and integrating a flip-flop–based clock gating technique. The objective is to enhance both security and power efficiency while maintaining system performance.

2. LITERATURE SURVEY

Several research works have been carried out to improve the performance and efficiency of AES hardware implementations. Researchers have mainly focused on optimizing functional blocks such as S-Box, MixColumns, and key expansion to reduce area, delay, and complexity.

M. Rajeswara Rao et al. proposed a combined S-Box and inverse S-Box architecture to reduce hardware complexity and memory usage. Nalini C. Iyer et al. introduced an optimized MixColumn design using resource sharing techniques to improve hardware efficiency. Yulin Zhang et al. developed a pipelined AES architecture to enhance throughput and reduce delay.

Other approaches include high-speed AES implementations and hardware optimization techniques such as parallel processing and lookup table optimization. These methods improve performance but often increase power consumption.

Despite these improvements, most existing designs do not adequately address power efficiency. Continuous clock activity leads to increased dynamic power consumption, making power optimization a critical requirement in modern AES implementations.

3. EXISTING SYSTEM

The existing system is based on AES-128, which operates on a 128-bit data block with a 128-bit key. AES is a symmetric-key block cipher standardized by NIST, and it is considered more secure than DES due to its larger key size and resistance to brute-force attacks. DES, with a 56-bit key,

has become vulnerable, leading to the adoption of AES for modern applications.

In AES-128, the encryption process consists of 10 rounds, where each round performs SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations. Round keys are generated from the original key using a key expansion algorithm, ensuring that each round uses a unique key. The block diagram of AES is illustrated in Figure 1. In conventional implementations, all modules are driven by a continuous clock signal, regardless of their activity. This leads to unnecessary switching in idle components, resulting in increased dynamic power consumption and inefficient utilization of hardware resources.

Limitations: The existing AES-128 system suffers from high power consumption due to continuous clocking of all modules, leading to unnecessary switching activity. It also inefficiently utilizes hardware resources, making it less suitable for lowpower and embedded applications.

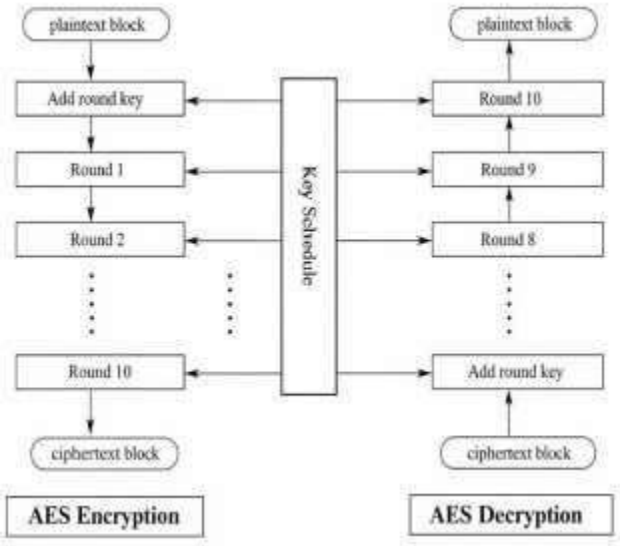

Fig. 1: Block Diagram of Advanced Encryption Standard (AES)

4. PROPOSED SYSTEM

To overcome the limitations of the existing system, a power-efficient AES architecture is proposed using AES-256. The proposed system operates on a 128-bit data block with a 256-bit key and performs 14 rounds of encryption, providing enhanced security. The encryption process includes SubBytes, which performs non-linear substitution using an S-Box; ShiftRows, which cyclically shifts the rows of the state matrix; MixColumns, which applies a linear transformation to each column; and AddRoundKey, which combines the state matrix with round keys.

An efficient key expansion mechanism is used to generate round keys for each stage of encryption. In addition, a flip-flop–based clock gating technique is integrated to reduce dynamic power consumption by disabling the clock signal to inactive modules. By combining AES-256 encryption with clock gating, the proposed system improves both security and power efficiency. The design is verified through simulation and evaluated based on power, delay, and hardware utilization. Figures 2 and 3 illustrate the block diagram of the AES algorithm and its flip-flop-based clock gating implementation, respectively.

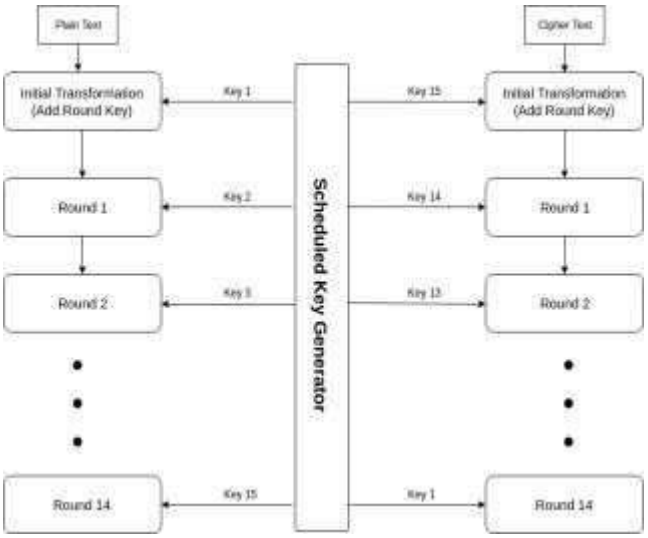

Fig. 2: Block Diagram of AES

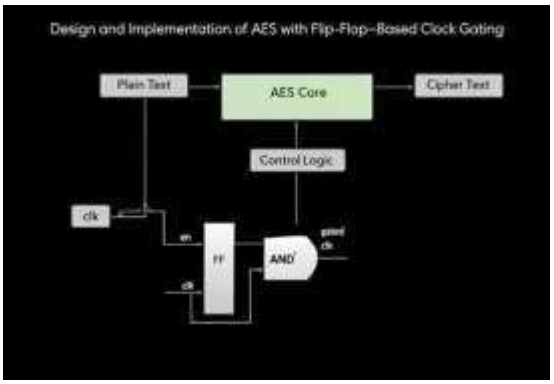

Fig. 3: Block Diagram for AES with Flip-flop Based Clock Gating

5. IMPLEMENTATION AND RESULTS

The proposed AES architecture is implemented using Verilog HDL and verified through simulation. Both the existing AES-128 and proposed AES-256 systems are analyzed and compared based on performance parameters such as power consumption, delay, and hardware utilization.

The simulation results confirm the correct functionality of the encryption process, including all transformation stages. The proposed system demonstrates reduced switching activity due to the integration of clock gating, which minimizes unnecessary clock distribution. Figs. 4–11 show the simulation waveforms, power consumption, FPGA resource utilization, and timing analysis for the existing and proposed AES implementations with 128bit and 256-bit keys.

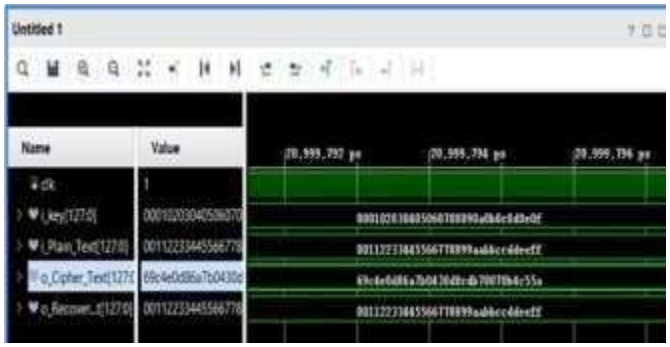

Fig. 4: Simulation Waveform of AES Existing System Encryption Process

Fig. 5: Power Consumption AES 128 bits key

Name	Slice LUTs (134600)
AES_TOP	16916
dec_inst (decryption)	5357
enc_inst (encryption)	11559

Fig. 6: FPGA Resource Utilization for AES_128bits Implementation

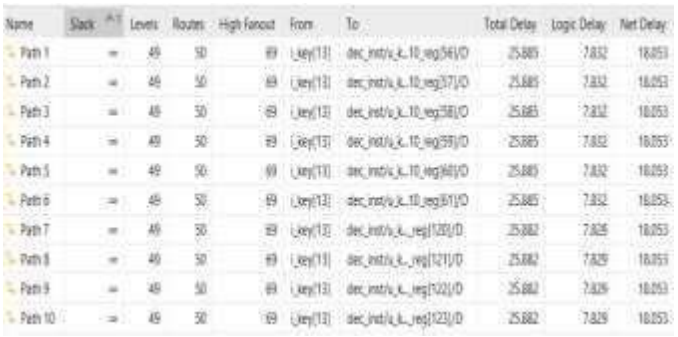

Fig. 7: Timing Analysis Report of AES-128bits Encryption/Decryption

Fig. 8: Simulation Waveform of AES Proposed System Encryption Process

Fig. 9: Power Consumption AES 256 bits key

Name	Slice LUTs (134600)
AES_TOP_256_EXTENSION	22608
dec_inst (decryption_256)	9783
enc_inst (encryption_256)	12824

Fig. 10: FPGA Resource Utilization for AES_256bits Implementation

Name	Slack	Levels	Routes	High Fanout	From	To	Total Delay	Logic Delay	Net Delay
Path 1	∞	56	57	77	i_key[29]	enc_inst/u_k_14_reg[55]/D	28.504	9.727	18.777
Path 2	∞	56	57	77	i_key[29]	enc_inst/u_k_14_reg[86]/D	28.504	9.727	18.777
Path 3	∞	56	57	77	i_key[29]	enc_inst/u_k_14_reg[87]/D	28.504	9.727	18.777
Path 4	∞	56	57	77	i_key[29]	enc_inst/u_k_14_reg[22]/D	28.501	9.724	18.777
Path 5	∞	56	57	77	i_key[29]	enc_inst/u_k_14_reg[23]/D	28.501	9.724	18.777
Path 6	∞	56	57	77	i_key[29]	enc_inst/u_k_14_reg[54]/D	28.501	9.724	18.777
Path 7	∞	56	57	77	i_key[29]	enc_inst/u_k_14_reg[16]/D	28.477	9.724	18.753
Path 8	∞	56	57	77	i_key[29]	enc_inst/u_k_14_reg[17]/D	28.477	9.724	18.753
Path 9	∞	56	57	77	i_key[29]	enc_inst/u_k_14_reg[18]/D	28.477	9.724	18.753
Path 10	∞	56	57	77	i_key[29]	enc_inst/u_k_14_reg[19]/D	28.477	9.724	18.753

Fig. 11: Timing Analysis Report of AES_256bits Encryption/Decryption

6. DISCUSSION

The comparative analysis shows that the proposed system achieves lower power consumption compared to the existing system while maintaining similar delay and hardware efficiency. The increase in key size further enhances the security of the encryption process.

7. CONCLUSION

Table-1: Comparison of Existing and Proposed Method

Parameter	Existing System	Proposed System
Power (W)	1836.566	772.743
Delay(ns)	25.885	28.504
Area (LUTs)	16916	22608

This work presents a power-efficient AES architecture supporting both 128-bit and 256-bit key sizes, implemented using Verilog HDL and analyzed in Xilinx Vivado. The proposed design achieves a substantial power reduction from 1836.566 W to 772.743 W without affecting delay, ensuring efficient operation. Additionally, the use of a 256-bit key with 14 rounds enhances security against brute-force attacks.

The use of flip-flop–based clock gating minimizes unnecessary switching activity, resulting in improved energy efficiency without affecting system performance. The proposed design is suitable for secure and low-power cryptographic applications.

ACKNOWLEDGEMENT

The authors sincerely thank Ms. M. Pavitra (Associate Professor, ECE, PBR VITS Kavali) for his guidance, Dr. R. Sravanthi (Professor &HoD, ECE) for providing facilities, and Dr. V. Anil Kumar (Principal, PBR VITS Kavali) for the academic environment that enabled this work.

REFERENCES

[1] M. Rajeswara Rao, Dr.R.K.Sharma, SVE Department, NIT Kurushetra "FPGA Implementation of combined S box and Inv S box of AES" 2017 4th International conference on signal processing and integrated networks (SPIN).

[2] Nalini C. Iyer; Deepa; P.V. Anandmohan; D.V. Poornaiah "Mix/Inv Mix Column decomposition and resource sharing in AES".

[3] Yulin Zhang; Xinggang Wang; "Pipelined implementation of AES encryption based on FPGA" 2010 IEEE International Conference on Information Theory and Information Security.

[4] C. Sivakumar; A. Velmurugan; "High Speed VLSI Design CCMP AES Cipher for WLAN (IEEE 802.11i)" 2007 International Conference on Signal Processing, Communications and Networking.

[5] P. S. Abhijith; Mallika Srivastava; Aparna Mishra; Manish Goswami; B. R. Singh; "High performance hardware implementation of AES using minimal resources" 2013 International Conference on Intelligent Systems and Signal Processing (ISSP).

[6] N. S. Sai Srinivas; Md. Akramuddin; "FPGA based hardware implementation of AES Rijndael algorithm for Encryption and Decryption" 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT).

[7] Ashwini M. Deshpande; Mangesh S. Deshpande; Devendra N. Kayatanavar; "FPGA implementation of AES encryption and decryption" 2009 International Conference on Control, Automation, Communication and Energy Conservation.

[8] Shady Mohamed Soliman, Baher Magdy and Mohamed A. AbdE1 Ghany, "Efficient implementation of the AES algorithm for security applications", IEEE 2016.

[9] J. Daemen and V. Rijmen, The block cipher Rijndael, Smart Card research and Applications, LNCS 1820, Springer-Verlag, pp. 288-296.

[10] Jamal, K., Srihari, P., &Kanakasri, G. (2016). Test Vector Generation using Genetic Algorithm for Fault Tolerant Systems. International Journal of Control Theory and Applications (IJCTA), 9(12), 5591-5598.

[11] Mohini Mohurle and Vishal V. Panchbhai, "Review on realization of AES encryption and decryption with power

and area optimization",1st IEEE Conference on power electronics, intelligent control and energy system (ICPEICES-2016).