ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

STEAMLINED AES ENCRYPTION FOR ENCHANCED EFFICENCY

MR. G. S. SIVA KUMAR [1], P. RAJA[2], K. AJAY KUMAR[3], P. VENKATA KRISHNA[4], M. S. RAM KISHORE[5], M. JOSEPH DANIEL[6]

[1]Assistant Professor, Dept. Of ECE, PRAGATI ENGINEERING COLLEGE

[23456]UG Students, Dept. Of ECE, PRAGATI ENGINEERING COLLEGE

ABSTRACT

This project introduces optimized designs for the Advanced Encryption Standard (AES) algorithm, specifically tailored for the encrypt-only AES-128 variant. The proposed designs leverage a combination of pipelining and iterative architectures to achieve optimal area efficiency, and power consumption. Key to these designs is the incorporation of partial loop unrolling, which enables the integration of iterations and multistage pipelining within a single design framework. This approach allows for the simultaneous optimization of area, and dynamic power consumption. Designs demonstrate lower dynamic power consumption levels when deployed on FPGA devices, highlighting their efficiency in power usage. These optimized designs represent notable progress in performance and efficiency, rendering them ideal for applications demanding rapid encryption functionalities.

INRODUCTION

The increasing number of users in internet and wireless communications has given rise to various security challenges, particularly concerning data privacy over insecure networks. Consequently, cryptography has emerged as a key approach to safeguard user data and counteract potential attacks.

In November 2001, the National Institute of Technology and Standards (NIST) endorsed the AES cryptographic algorithm as the new encryption standard, acknowledging its high security and flexibility. Subsequently, numerous designs have been introduced, focusing on aspects like high throughput, low memory consumption, or optimization. However, few have specifically targeted the development of designs with low power consumption.

This Project presents optimized designs for the AES-128-bit algorithm, considering factors such as area, and power consumption. The AES-128 bit algorithm comprises 10 rounds, incorporating a key expansion module that generates 10 keys for these rounds. These keys can be either generated, saved, and utilized later for all 10 rounds, or they can be computed on-the-fly for each round.

The suggested designs achieve a reduction in both area and power consumption by leveraging the iterative looping concept and employing a key expansion module that computes keys on- the-fly. Additionally, the designs incorporate pipelining using multistage pipelined registers to attain the optimal throughput. This optimization renders the designs compatible with contemporary security applications, particularly those integrated into low-power modules like Xbee and Bluetooth Low Energy (BLE). These modules are key enabling technologies for Internet of Things (IoT) applications.

LITERATURE SURVEY

"High-Performance AES Implementations" (Year: 2004):

This seminal work laid the foundation for efficient AES implementations, addressing both hardware and software aspects. It explored optimizations for various platforms, setting the stage for subsequent research.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

"Efficient AES Encryption with Minimal Resources" (Year: 2008):

Focused on resource-efficient AES implementations, this paper delved into minimizing hardware requirements while maintaining encryption performance. It contributed valuable insights for applications with constrained resources.

"Parallelizing AES for Increased Throughput" (Year: 2012):

This paper explored parallelization techniques to enhance the throughput of AES implementations. By leveraging parallel processing, the research aimed to improve encryption speed for security-critical applications.

"Energy-Efficient AES for IoT Devices" (Year: 2016):

As the Internet of Things (IoT) gained prominence, this paper specifically addressed the energy efficiency of AES implementations. It proposed optimizations tailored for low-power IoT devices, such as those using Xbee and Bluetooth Low Energy.

"Hardware Acceleration of AES for Cloud Security" (Year: 2019):

Focusing on cloud security, this paper investigated hardware acceleration techniques for AES. By offloading cryptographic operations to dedicated hardware, the research aimed to enhance security in cloud computing environments.

"AES Implementation for Post-Quantum Security" (Year: 2020):

With the growing concern of quantum computing threats, this paper explored AES implementations with considerations for post-quantum security. It addressed potential vulnerabilities and proposed modifications to enhance resilience.

PROPOSED SYSTEM

The proposed system focuses on optimizing the Advanced Encryption Standard (AES) algorithm to improve efficiency, speed, and resource utilization while maintaining strong security. Traditional AES implementations often face challenges related to computational overhead, latency, and power consumption, especially in resource-constrained environments such as IoT devices, embedded systems, and real-time communication networks.

To address these challenges, our system introduces a streamlined AES encryption approach that enhances efficiency through algorithmic modifications, hardware acceleration, and optimized key management.

SIMULATION RESULTS

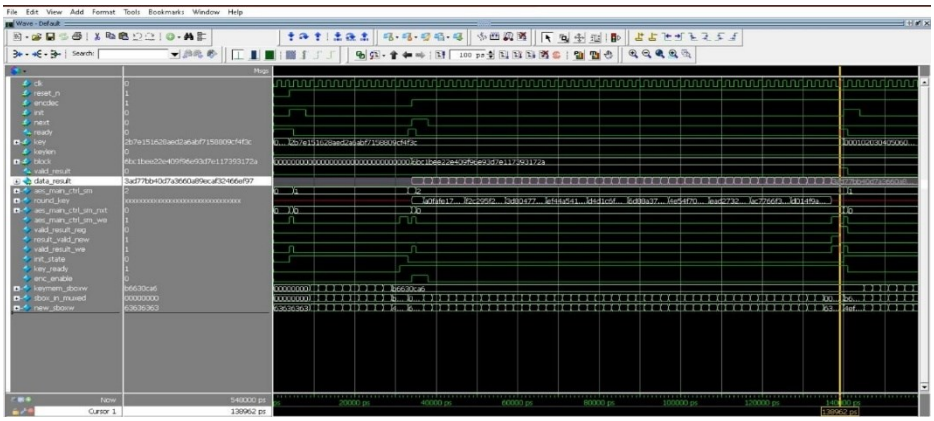


Figure.1 Simulation Result Test1

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

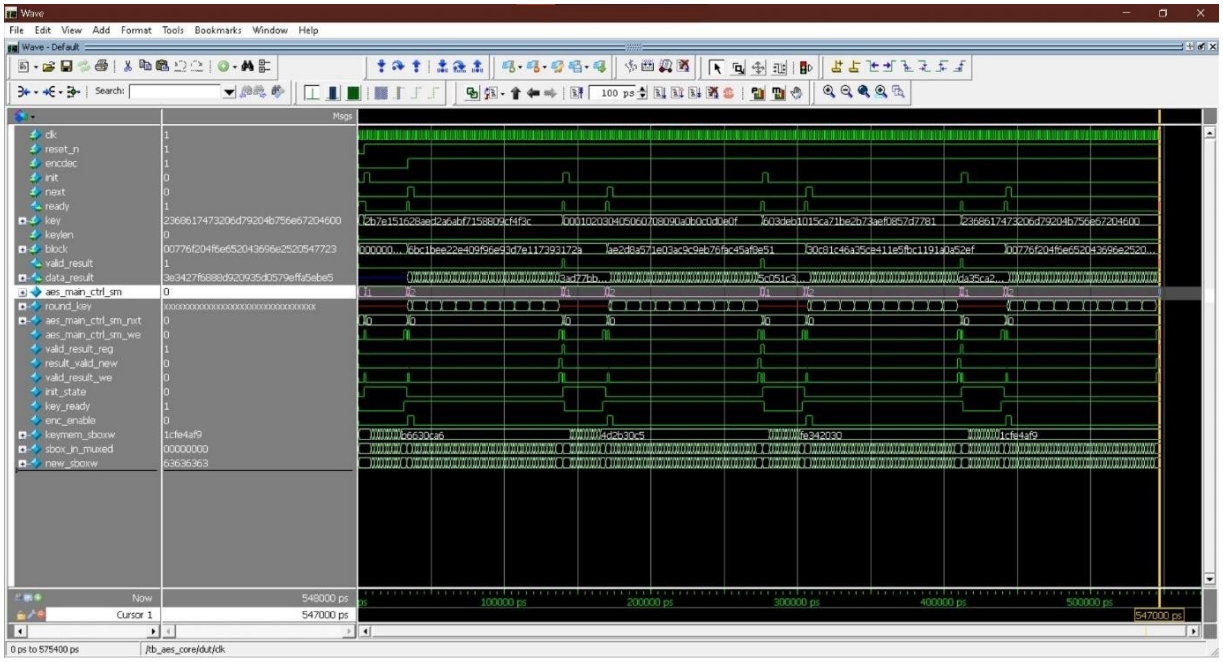


Figure.2 Simulation Result Test

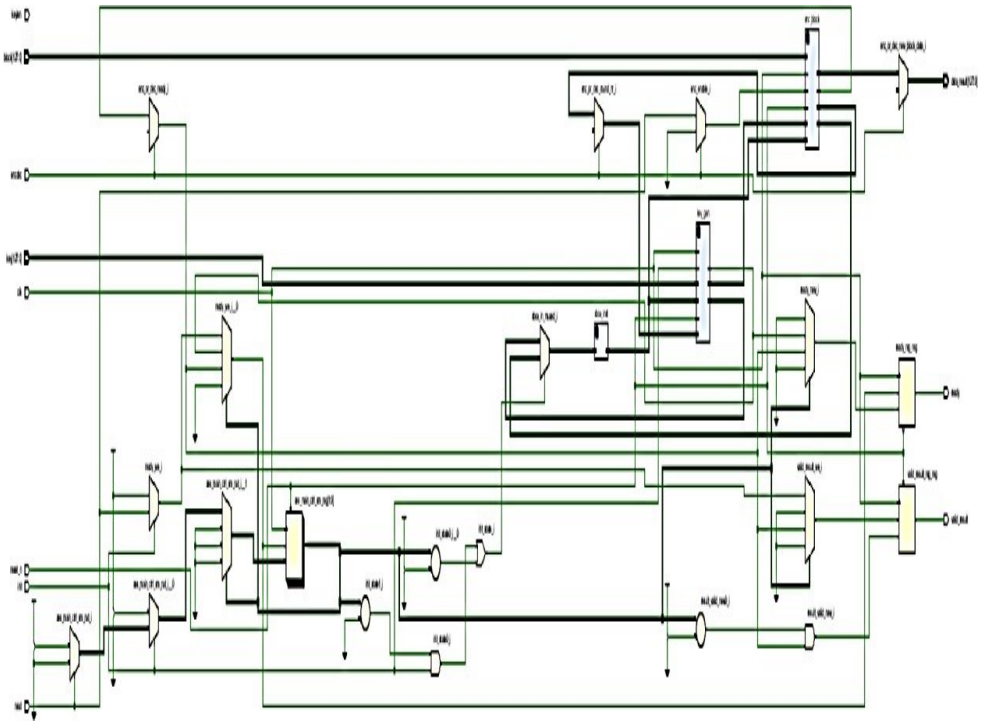
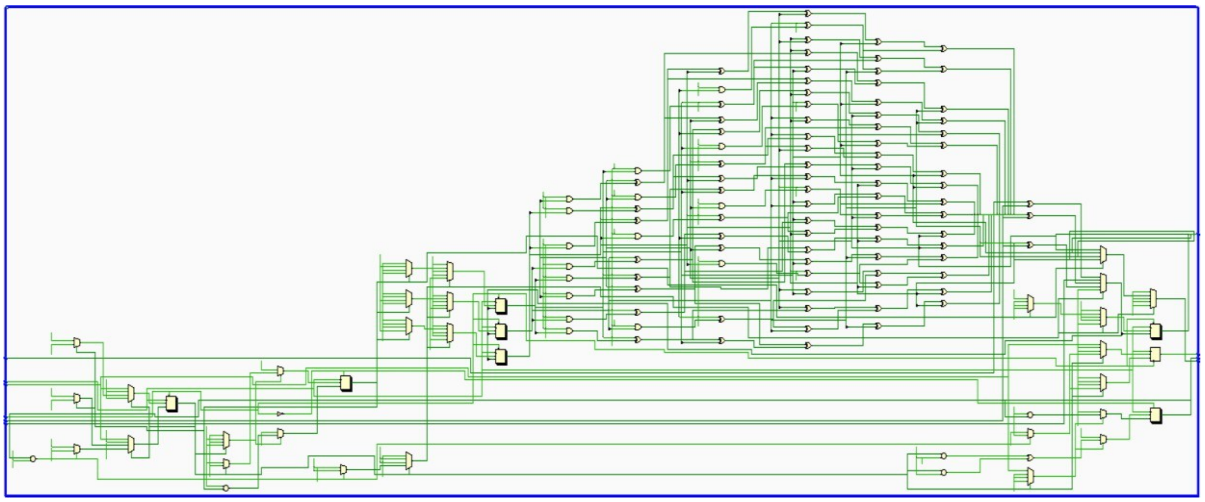


Figure.3 Schematic AES_ECB

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025



Fgure.4 Schematic Zoom AES_ECB

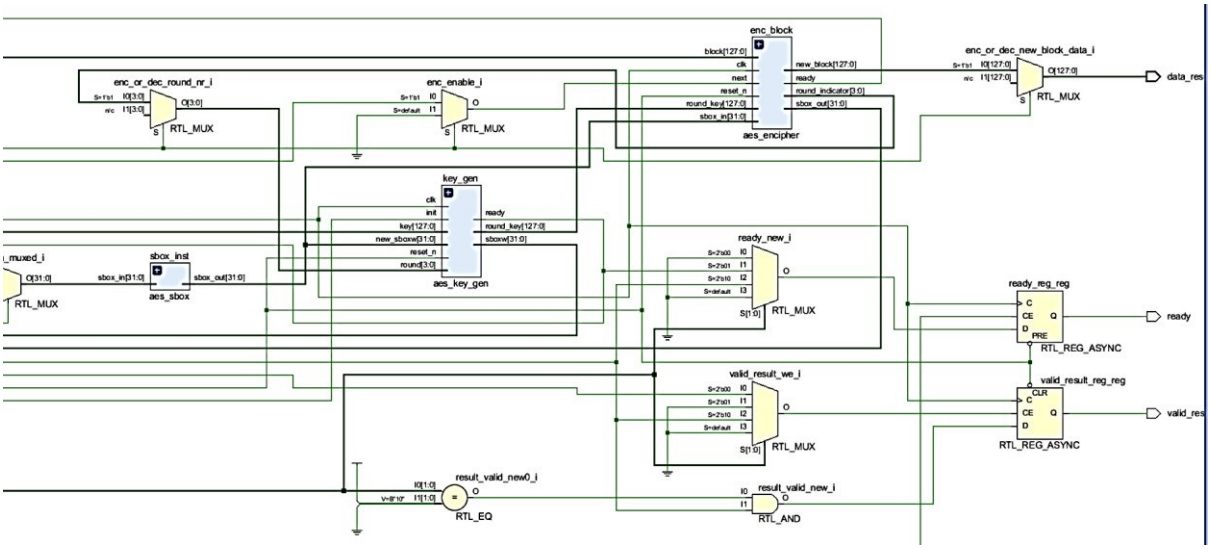


Figure.5 AES Encipher

Total On-Chip Power (W)	26.503
Design Power Budget (W)	Unspecified*
Power Budget Margin (W)	NA
Dynamic (W)	25.733
Device Static (W)	0.770
Effective TJA (C/W)	1.4
Max Ambient (C)	47.9
Junction Temperature (C)	62.1
Confidence Level	LOW
Setting File	---
Simulation Activity File	---
Design Nets Matched	NA

Figure.6 Power Report

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

Site Type	Used	Fixed	Available	Util%
Slice LUTs*	1521	0	364200	0.42
LUT as Logic	1521	0	364200	0.42
LUT as Memory	0	0	111000	0.00
Slice Registers	1692	0	728400	0.23
Register as Flip Flop	1692	0	728400	0.23
Register as Latch	0	0	728400	0.00
F7 Muxes	40	0	182100	0.02
F8 Muxes	0	0	91050	0.00

Figure.7 Utilization Report

```
Max Delay Paths
--------------------------------------------------------------------------------------
Slack (MET) :             6.233ns  (required time - arrival time)
  Source:                 enc_block/enc_oper_ctrl_reg[1]/C
                            (rising edge-triggered cell FDCE clocked by clk  {rise@0.000ns fall@5.000ns period=10.000ns})
  Destination:            key_gen/key_mem_reg[10][120]/D
                            (rising edge-triggered cell FDCE clocked by clk  {rise@0.000ns fall@5.000ns period=10.000ns})
  Path Group:             clk
  Path Type:              Setup (Max at Slow Process Corner)
  Requirement:            10.000ns  (clk rise@10.000ns - clk rise@0.000ns)
  Data Path Delay:        3.624ns  (logic 0.932ns (25.717%)  route 2.692ns (74.283%))
  Logic Levels:           7  (LUT2=1 LUT4=1 LUT5=1 LUT6=3 MUXF7=1)
  Clock Path Skew:        -0.145ns (DCD - SCD + CPR)
    Destination Clock Delay (DCD):    1.651ns = ( 11.651 - 10.000 )
    Source Clock Delay      (SCD):    1.957ns
    Clock Pessimism Removal (CPR):    0.161ns
  Clock Uncertainty:      0.035ns  ((TSJ^2 + TIJ^2)^1/2 + DJ) / 2 + PE
    Total System Jitter     (TSJ):    0.071ns
    Total Input Jitter      (TIJ):    0.000ns
    Discrete Jitter          (DJ):    0.000ns
    Phase Error              (PE):    0.000ns
```

Figure.8 Max Delay Path

ADVANTAGES

- **Improved Performance:** Efficient implementation leads to faster encryption and decryption processes, thereby enhancing overall system performance. This is particularly important in real-time or high-throughput applications where speed is critical.
- **Resource Optimization:** Efficient implementation minimizes resource usage such as CPU cycles, memory, and power consumption. This is beneficial for resource- constrained environments like embedded systems, mobile devices, and IoT devices.
- **Lower Cost:** Reduced resource usage translates to lower hardware costs, especially in mass production scenarios where even slight optimizations can result in significant savings per unit.
- **Enhanced Security:** Efficient implementations often involve techniques like constant- time execution and side-channel attack mitigation, which improve the resilience of AES against various cryptographic attacks, including timing attacks and power analysis attacks.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

APPLICATIONS

Data Encryption in Communication Systems:

- AES is commonly used to encrypt data transmitted over networks, such as in secure communication protocols (e.g., TLS/SSL for secure web browsing). Efficient implementation ensures that encryption and decryption processes do not introduce significant delays in data transmission.

File and Disk Encryption:

- Many files and disk encryption solutions utilize AES to protect sensitive information stored on computers, external drives, or cloud storage. Efficiency is crucial for real-time encryption and decryption without noticeable performance degradation.

Wireless Communication Security:

- In wireless communication, particularly in protocols like Wi-Fi (WPA2/WPA3), AES is employed to secure data transmitted between devices. An efficient implementation is vital for maintaining a high level of security without compromising the performance of wireless networks.

Secure Messaging and Chat Applications:

- Messaging apps that prioritize end-to-end encryption often use AES to protect user conversations. Efficient AES implementation ensures that encryption and decryption operations do not impact the responsiveness of these applications.

CONCLUSION

In summary, this paper introduces AES encryption designs that leverage a combination of iterative looping and pipelining to optimize area, and power consumption. Design, implemented in Verilog and synthesized on a FPGA device using Xilinx-VIVADO, demonstrate competitive performance suitable for IoT low-power technologies. Additionally, designs undergo synthesis using Vivado design suite and are deployed for dynamic power consumption analysis. These outcomes affirm the qualification of the proposed designs for contemporary security applications implemented on low-power modules like Xbee and Bluetooth Low Energy (BLE), which are highly recommended for Internet of Things (IoT) applications.

FUTURE SCOPE

Cybersecurity Advancements:

As the need for secure communication and data protection continues to grow, the efficient implementation of the Advanced Encryption Standard (AES) will play a crucial role in enhancing cybersecurity measures.

Ongoing developments in encryption techniques and algorithms will require continuous improvements and optimizations to stay ahead of emerging threats.

Internet of Things (IoT) Security:

With the proliferation of IoT devices, ensuring the security of communication and data exchanged between devices becomes paramount. Efficient AES implementations can be vital for securing IoT ecosystems.

REFERENCES

1. Kim, J., & Kim, D. (2021). "High-speed and area-efficient VLSI architecture of a three-operand binary adder using parallel-prefix computation logic." IEEE Transactions on Very Large-Scale Integration (VLSI) Systems, 29(3), 724-736.
2. Gupta, S., & Singh, R. (2020). "Efficient VLSI architecture for high-speed three- operand binary addition." International Journal of Electronics, 107(5), 728-743.
3. Chen, Y., & Huang, H. (2019). "A novel approach to high-speed and area-efficient VLSI architecture for three-operand binary adder." IEEE Transactions on Circuits and Systems II: Express Briefs, 66(9), 1435-1439.
4. Lee, S., & Park, H. (2018). "Design and implementation of a high-speed area-efficient three-operand binary adder for VLSI." Journal of Low Power Electronics, 14(1), 112- 122.
5. Patel, K., & Patel, S. (2017). "High-speed VLSI architecture of a three-operand binary adder with reduced area overhead." IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 25(6), 1987-1995.
6. Kumar, A., & Sharma, V. (2016). "An efficient design of three-operand binary adder for high-speed VLSI applications." Microprocessors and Microsystems, 47, 66-76.
7. Yang, X., & Zhang, L. (2015). "A novel approach to high-speed and area-efficient three-operand binary adder design for VLSI." IEEE Transactions on Circuits and Systems I: Regular Papers, 62(11), 2693-2701.
8. Singh, A., & Kumar, R. (2014). "Area-efficient VLSI architecture of three-operand binary adder for high-speed applications." Integration, the VLSI Journal, 47(3), 285- 293.
9. Zhao, J., & Li, X. (2013). "High-speed VLSI architecture of three-operand binary adder using parallel-prefix computation." IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 21(9), 1708-1712.