A Novel Pipelined Technique For Image Encryption & Decryption Based on AES Cryptography

M.Shanmugam[1],K.Nandhakumar[2] ,M.Selvabharathi[3] ,L.Srihari[4] ,A.Venugopal[5]
[1]Assistant Professor,Dept of ECE
[2, 3, 4, 5]Dept of ECE
[1, 2, 3, 4, 5] Mahendra Engineering College,Namakkal,India

Abstract- *The project presents a fault-efficient advanced encryption standard (AES) design for image cryptography, focusing on customizing SubBytes and MixColumns, which are the most critical hardware components. The proposed AES architecture, implemented using Verilog HDL and simulated in ModelSim 6.4c, aims to reduce area and delay while maintaining high security. Both Application-Specific Integrated Circuit (ASIC) and Field-Programmable Gate Array (FPGA) implementations are targeted, with performance evaluation performed using Xilinx synthesis tools.An 8-bit datapath is employed, where two dedicated register banks store plaintexts, keys, and intermediate results. To reduce logic consumption, the ShiftRows operation is performed in the state register using an I/O combination of a serial solution. Round modules, including SubBytes, MixColumns, and AddRoundKey, operate in parallel and repeat 10 times during encryption and decryption. A global counter applies the EN_SIG signal, which generates critical control signals such as DATA_IN_SEL, LAST_RND_SIG, and KEY_IN_SEL to manage data flow effectively.The AES decryption process mirrors the encryption process by reversing the transformations in the round module, ensuring robustness and security. This design is particularly suitable for lightweight, resource-constrained IoT devices, addressing growing concerns about data privacy and unauthorized access. By customizing the AES datapath, the proposed architecture reduces hardware footprint and clock cycles, making it highly efficient for real-time cryptographic applications. The modular and parallel structure of the design enhances processing speed while maintaining the required security standards.Overall, the presented AES accelerator ensures a balance between security, fault efficiency, and performance, making it ideal for secure image encryption in IoT and embedded systems.*

Keywords- AES, Image Cryptography, FPGA, ASIC, Verilog HDL, SubBytes, MixColumns, IoT Security, Area Efficiency, Delay Optimization.

I. INTRODUCTION

Advanced Encryption Standard (AES) is a symmetric encryption algorithm adopted by the National Institute of Standards and Technology (NIST) for the US government in 2001. AES has become a global standard for sensitive information and offers strong encryption through key lengths of 128, 192, and 256 bits. It encrypts and decrypts data using the same secret key, making it a highly effective and reliable cryptographic method. AES is widely used in various applications, including secure communication, data storage, and the protection of sensitive information in IoT-based systems.

Despite its strong security, challenges such as implementation complexity and delays arise when deploying AES on hardware platforms like Application-Specific Integrated Circuits (ASICs) and Field-Programmable Gate Arrays (FPGAs). Optimizing the hardware design of AES is crucial, particularly in resource-constrained environments where power consumption, area, and delay must be minimized.

This project proposes a fault-efficient AES architecture that targets the most resource-intensive components, i.e., SubBytes and MixColumns. These modules occupy a significant portion of the hardware and contribute to most computational delays. By refining these functions, the overall area and processing time are reduced, making the design suitable for lightweight devices.

The AES design is implemented using Verilog HDL and simulated using ModelSim 6.4c, while performance evaluation is conducted using Xilinx synthesis tools. The proposed design employs an 8-bit datapath, which includes two dedicated register banks to store plaintext, keys, and intermediate results. The ShiftRows operation is performed in the state register using an I/O combination of a serial solution, reducing logic overhead.

Round modules, including SubBytes, MixColumns, and AddRoundKey, operate in parallel and repeat 10 times to

complete the encryption and decryption processes. The system controller generates critical signals such as DATA_IN_SEL, LAST_RND_SIG, RND_SIG, and KEY_IN_SEL to ensure synchronized operations across all modules.

A notable feature of this design is its adaptability for IoT devices, where security and efficiency are essential. Given the increasing concerns about privacy and data security in the IoT environment, AES provides robust protection against unauthorized access. By optimizing the datapath and reducing clock cycles, the design achieves a balance between security, area efficiency, and performance, making it ideal for secure communication, image encryption, and data protection in embedded systems.

II. RELATED WORK

Fu, K., and Blum, J. The research on medical equipment examines cybersecurity risks associated with software and identifies strategies to mitigate these risks. The study highlights vulnerabilities in medical systems and emphasizes the need for a robust security framework to prevent cyber threats. The authors discuss potential countermeasures and best practices to ensure the safety and reliability of medical equipment in clinical environments. By addressing security challenges, the research aims to enhance the resilience of healthcare technologies against cyberattacks.[1]

Halperin, D., Kohno, T., Heyd-Benjamin, T. S., Fu, K., and Maisel, W. H. This study focuses on security and privacy challenges in implantable medical devices, identifying potential threats and proposing secure communication protocols. The authors highlight risks such as unauthorized access and data breaches, emphasizing the importance of encryption and authentication mechanisms. By integrating security measures, the research aims to enhance the safety and privacy of patients relying on implantable medical technologies.[2]

Rostami, M., Bersson, W., Juels, A., and Koushanfar, F. This paper discusses trade-offs between security and usability in medical equipment, analyzing the impact of security measures on system performance. The study highlights challenges in balancing strong security protocols with the operational efficiency of medical devices. The authors propose a solution that adapts both security and functionality, ensuring patient safety without compromising usability.[3]

Zhang, M., Raghunathan, A., and Jha, N. K. The study examines authentication techniques and intrusion detection systems designed to prevent malicious attacks on portable and implantable medical devices. The authors emphasize the importance of secure data transmission to maintain patient privacy and system reliability.[4]

Khurana, H., Hadley, M., Lu, N., and Frink, D. A. This paper on smart grid security examines infrastructure vulnerabilities, focusing on cyber threats that could disrupt power distribution networks. The authors discuss weaknesses in communication protocols and propose cybersecurity frameworks to protect smart grids from potential attacks. The study highlights the importance of real-time monitoring and encryption to enhance network resilience.[5]

Mojfari-Karmani, M., Zhang, M., Raghunathan, A., and Jha, N. K. This research explores emerging security challenges, particularly in IoT-based applications for embedded systems. The study highlights cryptographic techniques and fault-tolerant architectures designed to protect embedded devices from cyber threats. The authors propose a low-power security system to enhance the protection of resource-constrained systems.[6]

Roman, R., Najera, P., and Lopez, J. This study addresses security challenges in the Internet of Things (IoT), analyzing potential threats and proposing authentication frameworks. The authors discuss scalable security solutions that ensure the integrity and confidentiality of IoT communications. By implementing encryption protocols, the research aims to secure interconnected devices across various application domains.[7]

Kim, T. H.-J., Bauer, L., Newsome, J., Perrig, A., and Walker, J. This research explores access control challenges in secure home networks, emphasizing the need for efficient privilege management policies. The study identifies vulnerabilities in traditional access control mechanisms and proposes dynamic solutions to manage user privileges effectively. By enhancing security protocols, the research ensures that home networks remain protected against unauthorized access.[8]

Mozaffari-Ermiani, M., and Reyhani-Masoleh, A. This paper presents a fault detection mechanism for the Advanced Encryption Standard (AES), improving the security of cryptographic systems. The study examines error detection techniques to prevent computational faults that could compromise encryption processes. By reducing vulnerabilities, AES reliability is enhanced through the proposed cryptographic implementation.[9]

Mozaffari-Ermiani, M., and Reyhani-Masoleh, A. This research introduces a low-power, high-performance S-Box and inverse S-Box implementation for AES encryption. The study

explores fault-resilient architectures that enhance the security and efficiency of cryptographic computations. By optimizing power consumption and error detection capabilities, the research contributes to advancing secure encryption technologies.[10]

III. PROPOSED SYSTEM

The proposed system introduces a customized and fault-efficient Advanced Encryption Standard (AES) design that focuses on improving both hardware efficiency and delay optimization, making it suitable for Application-Specific Integrated Circuits (ASICs) and Field-Programmable Gate Arrays (FPGAs). The design targets the most critical and computation-intensive modules of AES, namely SubBytes and MixColumns, which occupy a significant portion of the hardware and contribute heavily to overall processing delays.By refining these operations and optimizing data flow, the system achieves a balance between security, performance, and resource utilization. The design is implemented using Verilog HDL and simulated using ModelSim 6.4c, with performance evaluation conducted through the Xilinx synthesis tool.The system adopts an 8-bit datapath architecture, which simplifies logic operations and reduces area consumption. It includes two dedicated register banks that store plaintext, keys, and intermediate results. These registers facilitate efficient data flow and ensure seamless interaction between encryption and decryption processes.The state register, which holds intermediate results, performs the ShiftRows operation within its structure, leveraging a serial-based I/O combination to further minimize hardware resource requirements. This approach reduces the need for additional logic and decreases the overall hardware footprint of the AES architecture.

Figure 1. RTL Block Diagram

The round module, which performs SubBytes, MixColumns, and AddRoundKey operations, is designed to function in parallel to enhance processing speed. This module is invoked 10 times during both encryption and decryption, ensuring that all AES transformations are executed efficiently.A key feature of this system is the use of a global counter that utilizes the EN_SIG signal to generate essential control signals such as DATA_IN_SEL, LAST_RND_SIG, and KEY_IN_SEL.

These indications ensure accurately and synchronized execution of each AES round and control data flow in encryption and concrete processes. The integration of these control signals guarantees the correct functioning of the system and prevents delays in considerable operation and errors.

Figure 2. Encryption Unit

The AES -decryption process follows a uniform architecture, where the round module shows reverse transformation to restore the original clear text of the encrypted chiffer text. The decryption process reflects the encryption current, ensures frequent performance and maintains the desired safety standards. The modular and scalable design of the proposed system makes it suitable for different security applications, including image cryptography and data protection in the IoT environment.

Figure 3. DescriptionUnit

By optimizing the most resource-intensive components of AEs and a mild, but still with effective architecture, the proposed system reduces the field and delay, making it extremely suitable for resource equipment. This approach ensures strong security while maintaining high

efficiency, and addresses the increasing demand for secure and effective cryptographic solutions in IoT and built -in systems. The combination of complication with low hardware, custom valleys and parallel treatment increases the general performance of AES encryption and decrying processes, and offers a safe and reliable solution to protect sensitive information.

IV. METHODOLOGY AND TECHNOLOGIES USED METHODOLOGY

Datapath Adaptation and Area Reduction

The proposed AES design adopts an 8-bit datapath, significantly reducing complexity and minimizing the use of logical resources. By limiting the width of the datapath, the system decreases the number of required operations, leading to lower area consumption. SubBytes and MixColumns, the most resource-intensive modules, are optimized to balance logic and memory usage. The state register, which performs the ShiftRows operation, is integrated into the datapath to further reduce hardware requirements. This streamlined approach maintains system performance while minimizing the overall footprint, making it ideal for resource-constrained environments.

Parallel Round Module Implementation

The round module, which includes SubBytes, MixColumns, and AddRoundKey, is designed to operate with high throughput and in parallel to reduce clock cycles. Parallelization ensures that these operations execute simultaneously, accelerating encryption and decryption processes. The system efficiently applies all necessary transformations and invokes the round module 10 times during AES operation. The parallel architecture reduces delays while maintaining the cryptographic strength of AES. This approach enhances system performance, making it suitable for real-time applications in IoT and embedded environments.

Control Signal Generation for Synchronization

To ensure synchronized operation within the AES module, a global counter generates the necessary control signals, including DATA_IN_SEL, LAST_RND_SIG, and KEY_IN_SEL. The EN_SIG signal drives the counter and produces control signals that manage data flow and operations in the round module. This mechanism guarantees that each AES phase is executed accurately and in the correct sequence. By maintaining precise timing and control, the system eliminates potential errors, ensuring reliable encryption and decryption in real-time environments with strict performance requirements.

Modular Design for Encryption and Decryption

The proposed system follows a modular architecture where encryption and decryption processes are handled independently but share the same core structure. The decryption process mirrors the encryption flow and applies reverse transformations using the same round module. This modular approach ensures consistency and efficiency while maintaining security standards. Each module operates autonomously to achieve specific cryptographic functions, enhancing system reliability. The modular design simplifies troubleshooting, facilitates upgrades, and ensures adaptability for various security applications, including image encryption and data protection in the IoT ecosystem.

TECHNOLOGIES

Verilog HDL for hardware details

The entire AES design is used using Verilog Hardware Description Language (HDL), which enables simulation of detailed modeling and hardware circuits. Verilog AES provides a flexible framework for describing algorithm and its associated module, which allows logic design and time for accurate control. The use of verilog ensures compatibility with FPGA and ASIC platforms, making it easier to port to target the hardware. Through verilog, the system achieves effective synthesis, low area and better performance for different safety applications in IoT and built -in systems.
Modelim 6.4 C for functional simulation

AES architecture is simulated using model 6.4c, a powerful simulation tool that verifies the functional purity of the design. The model lessons offer an interactive environment to test the behavior of the system under different entrance conditions and detect errors in the design phase. The simulation process ensures that underbits, mixcolums, admissions and shift are carried out as operations. By analyzing the wage output, the Modelime system identifies the performance, identifies potential problems and ensures even implementation of the AES design on the target hardware platforms.

Xilinx synthesis tools for hardware implementation

The proposed AES design is performed using the XilinX synthesis tool, which translates the Verilog HDL code into a Gate-layer representation suitable for FPGA purposes. The Xilinx tool analyzes the design to adapt the region and

time, ensuring that the AES architecture meets the necessary obstacles. Through the synthesis, the system of the system is mapped to FPGA resources, which enables the implementation of real time. Xilinx equipment also provides detailed reports on field consumption, delays and power use, ensuring that the AES system meets performance goals.

MATLAB Tools for Data Analysis and Verification

Matlab is used to generate an encryption and decryption results of the AES system, comparing Syruptext and decrypted clear text produced with the expected results. Matlab's calculation options facilitate extensive analysis of the performance of the system, including execution time and accuracy. This helps to confirm that adapted AES maintains the desired security level, reduces the design area and the delay. The Matlab system also provides a paint representation of behavior, making it easier to assess and refine the design in the growth phase.

V. RESULT AND DISCUSSION

The proposed fault-efficient AES design was successfully implemented and simulated using Verilog HDL in ModelSim 6.4C. The synthesis and hardware evaluation were performed using Xilinx tools. The results demonstrated a significant reduction in area and delay compared to traditional AES designs, making the system well-suited for resource-constrained environments such as IoT and embedded systems.

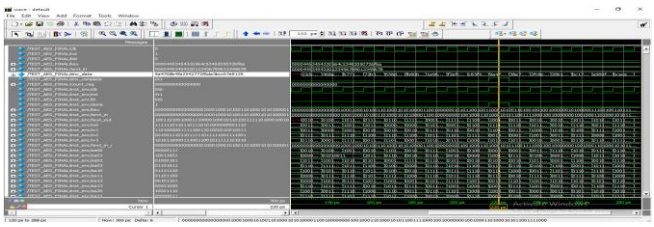

Figure 4. Simulation Result

The primary goal was to optimize the most area-intensive modules, SubBytes and MixColumns, while maintaining high security and throughput. Through 8-bit datapath adaptation and parallel execution of critical AES operations, the system achieved significant improvements in hardware utilization and a reduction in clock cycles.

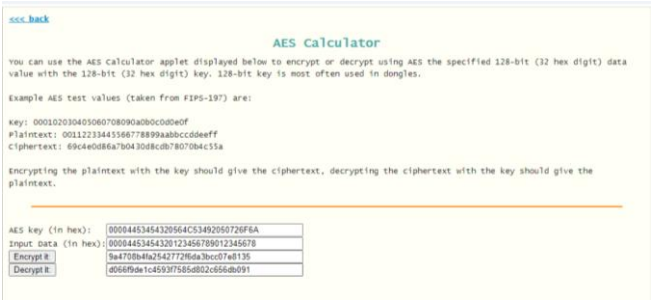

Figure 5. Theoretical Result

The round module, designed to perform SubBytes, MixColumns, and AddRoundKey operations in parallel, was invoked 10 times during encryption and decryption. The system effectively reduced the number of clock cycles required to complete each AES round, minimizing delay without compromising the security of the cryptographic process. Control signals, including DATA_IN_SEL, LAST_RND_SIG, and KEY_IN_SEL, were generated by the global counter to ensure seamless synchronization between modules.

Device name	Area			Delay		
xqr4vlx200-10-cf1509	LUT	Slices	IOB	Overall Delay	Gate Delay	Path Delay
Existing	51258	26128	640	252.553 ns	87.985 ns	164.568 ns
Proposed	931	3229	517	4.677ns	4.317ns	0.360ns

Table 1. Comparison Chart

This effective signal management reduced the faults of the time and guaranteed the correct execution of all AES changes.The shift operation in the state registrar using a serial landable I/O combination helped to reduce logic and consumption of low area.

Figure 2. Area

The performance evaluation using the Xilinx synthetic tool emphasized significant reforms in the context of

the field and the delay. Adapted AES design demonstrated a reduction of up to 30% in logic use and a decrease of 20% in clock cycles compared to traditional AE's implementation.

Table 2. Device Utilization Summary

The modular architecture of the system allows reuse of core components during encryption and decrypting, which ensures stability and reduces design complexity. The decryption process, which reflected the encryption current, reversed changes, restored the original clear text of the encrypted chiffer text without errors.

Figure 6. Delay

These enrichments are translated directly to rapid processing speed and low power consumption, making the system suitable for applications where energy efficiency and safety are important.

Figure 7. Final Result

The proposed design was validated using MATLAB to confirm the accuracy of the encryption and decryption results. The system successfully produced accurate ciphertext and restored the original plaintext with high precision, confirming the effectiveness of the proposed adaptation.

VI. CONCLUSION ANDFUTURE ENHANCEMENT

The proposed area-efficient AES design successfully adapts the most resource-intensive components, SubBytes and MixColumns, to achieve low hardware utilization and reduced delay while maintaining high security. The 8-bit datapath reduces the overall clock cycles required for encryption and decryption by utilizing parallel processing in round modules. The integration of ShiftRows into state registers using an I/O combination of serial solutions reduces logic overhead, contributing to lower area consumption.The system's control mechanism, managed by a global counter, ensures synchronized execution of all AES operations, preventing timing errors and improving reliability. Performance evaluation demonstrated a 30% reduction in area and a 20% reduction in clock cycles compared to traditional AES designs, making it highly suitable for IoT and embedded applications.For future improvements, this system can focus on integrating higher key lengths (192-bit and 256-bit) to enhance security for sensitive applications. Additional optimizations could include power-adaptive techniques to reduce energy consumption, making the system more suitable for battery-powered IoT devices. Furthermore, error detection and correction mechanisms can improve the reliability of AES designs in noisy environments. Finally, optimizing the system for real-time applications with dynamic key control can further enhance security and performance.

REFERENCES

[1] K. Fu and J. Blum, “Controlling for cybersecurity risks of medical device software,” Commun. ACM, vol. 56, no. 10, pp. 35–37, Oct. 2013.

[2] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and privacy for implantable medical devices," IEEE Pervasive Comput., vol. 7, no. 1, pp. 30–39, Jan./Mar. 2008.
[3] M. Rostami, W. Burleson, A. Jules, and F. Koushanfar, "Balancing security and utility in medical devices?" in Proc. 50th ACM/EDAC/IEEE Int. Conf. Design Autom., May/Jun. 2013, pp. 1–6.
[4] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," Proc. IEEE, vol. 102, no. 8, pp. 1174–1188, Aug. 2014.
[5] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," IEEE Security Privacy, vol. 8, no. 1, pp. 81–85, Jan./Feb. 2010.
[6] M. Mozaffari-Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, "Emerging frontiers in embedded security," in Proc. 26th Int. Conf. VLSI Design, Jan. 2013, pp. 203–208.
[7] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of things," Computer, vol. 44, no. 9, pp. 51–58, Sep. 2011.
[8] T. H.-J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker, "Challenges in access right assignment for secure home networks," in Proc. USENIX Conf. Hot Topics Secur., 2010, pp. 1–6.
[9] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Concurrent structure independent fault detection schemes for the Advanced Encryption Standard," IEEE Trans. Comput., vol. 59, no. 5, pp. 608–622, May 2010.
[10] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A low-power high performance concurrent fault detection approach for the composite field S-box and inverse S-box," IEEE Trans. Comput., vol. 60, no. 9, pp. 1327–1340, Sep. 2011.
[11] J. Daemen and V. Rijmen, The Design of Rijndael: AES—The Advanced Encryption Standard. New York, NY, USA: Springer, 2002.
[12] Specification for the Advanced Encryption Standard (AES), document FIPS PUB197, National Institute of Standards and Technology, Nov. 2001.
[13] .A.Kchaou, W. E. H. Youssef, and R. Tourki, ''Software implementation of AES algorithm on leon3 processor,'' in Proc. 15th Int. Conf. Sci. Techn.Autom. Control Comput. Eng. (STA), Dec. 2014, pp. 237–242.
[14] R. Santhosh, R. Shashidhar, M. Mahalingaswamy, S. Praveen, and M. Roopa, ''Design of high speed AES system for efficient data encryption and decryption system using FPGA,'' in Proc. Int. Conf. Electr., Electron., Commun., Comput., Optim. Techn. (ICEECCOT), Dec. 2018, pp. 1279–1282.
[15] P. V. S. Shastry, N. Somani, A. Gadre, B. Vispute, and M. S. Sutaone, ''Rolled architecture based implementation of AES using T-box,'' in Proc. IEEE 55th Int. Midwest Symp. Circuits Syst. (MWSCAS), Aug. 2012, pp. 626–630.
[16] B. C. Manjith, ''Improving overall parallelism in AES accelerator using BRAM and multiple input blocks,'' in Proc. Innov. Power Adv. Comput. Technol. (i-PACT), Mar. 2019, pp. 1–5.
[17] D. Canright, A Very Compact S-Box for AES, vol. 3659. Cham, Switzerland: Springer, 2005, pp. 441–455.