International Journal of application or Innovation in engineering and management

Ijaiem.com/Mar 2025/ Volume 14/Issue 1/Article No-1/119-127
ISSN: 2319-4847

DESIGN AND ANALYSIS OF OPTIMIZED BLOCK CIPHER DESIGN

Mr. S. Shabbir Ali[1], G. V. Akshaya[2], G. Akkamma[3], S. Omkar[4], M. Brunda[5], B. Bharath Kumar[6]

[1] Research Supervisor, Assistant Professor, Dept. of ECE, ALTS, Ananthapuramu.

[2,3,4,5,6] UG Scholar, Dept. of ECE, ALTS, Ananthapuramu

Article Info

Received: 22-02-2025 Revised: 22 -03-2025 Accepted: 08-04-2025 Published:19/04/2025

ABSTRACT

This paper presents a novel block cipher architecture that integrates S-box and P-box structures to enhance encryption security and efficiency. Implemented using the Verilog hardware description language, the design is synthesized and evaluated on the Xilinx Vivado FPGA platform. The S-box and P-box components, which play a crucial role in ensuring strong cryptographic properties, are carefully optimized to achieve a balance between security and hardware efficiency. The proposed architecture is analyzed in terms of design methodology, implementation details, and performance metrics, including resource utilization and encryption strength. Experimental results demonstrate that the cipher achieves high security while maintaining efficient FPGA resource consumption. The findings underscore its potential for real-world applications requiring secure data encryption. This work contributes to the field of hardware-based cryptography by providing an optimized and scalable block cipher design suitable for various security applications.

Keywords: Block Cipher, S-box, P-box, Xilinx Vivado, Key Expansion, Verilog HDL, Encryption Algorithm

I. INTRODUCTION

Block ciphers serve as fundamental cryptographic building blocks, ensuring data security across various domains, including embedded systems, wireless networks, and IoT devices. In resource-constrained environments, designing efficient block ciphers that maintain a balance between strong security and minimal resource consumption is a critical challenge. Addressing this need, this paper presents a novel block cipher architecture that leverages S-box and P-box structures to enhance encryption strength while optimizing hardware efficiency. The cipher is implemented in Verilog and synthesized on the Xilinx Vivado FPGA platform, making it highly suitable for deployment in hardware- limited scenarios.

The security of the proposed cipher is significantly strengthened through the integration of an S-box, which introduces nonlinearity into the encryption process. This nonlinearity enhances the cipher's resistance to cryptanalysis techniques such as differential and linear cryptanalysis, making it more robust against attacks. In addition, a P-box is employed to improve diffusion by efficiently permuting bits, thereby ensuring that minor changes in plaintext lead to significant alterations in ciphertext. Efficiency is a key consideration in hardware implementations, particularly in embedded systems where power and resource constraints are crucial factors. The proposed block cipher is optimized to operate with low power consumption and high performance, making it ideal for lightweight cryptographic applications. Its design ensures secure encryption while maintaining minimal computational overhead, addressing the demands of modern security-critical systems. The architecture aligns with existing lightweight block ciphers such as PRESENT, KATAN, LED, Piccolo, and RECTANGLE, which are widely used in cyber-physical systems, IoT, and pervasive computing applications.

International Journal of application or Innovation in engineering and management

Ijaiem.com/Mar 2025/ Volume 14/Issue 1/Article No-1/119-127
ISSN: 2319-4847

II. EXISTING METHOD

Cryptographic techniques have undergone significant transformations, evolving from classical methods to sophisticated block ciphers that ensure secure communication in the digital age. Early encryption relied on simple substitution and transposition ciphers, such as the Caesar cipher and Vigenère cipher, which replaced or shifted characters within a message. The Rail Fence cipher and other transposition techniques rearranged message letters based on a pattern. While these methods provided basic security, they were highly vulnerable to frequency analysis, brute-force attacks, and cryptographic breakthroughs.

With the rise of mechanical encryption devices, cryptography became more complex. The Enigma machine, used extensively during World War II, applied multiple rotor-based substitutions to encode messages. However, Allied cryptanalysts successfully deciphered Enigma using techniques such as crib analysis and brute- force decryption. Similarly, the Hagelin cipher machines provided stronger encryption but were eventually broken due to advancements in computing and cryptanalysis.

The transition to digital cryptography led to the development of block ciphers, which encrypt fixed-size blocks of data rather than individual characters. The first widely adopted block cipher was the Data Encryption Standard (DES), introduced in 1977. DES is based on the Feistel network and operates through 16 rounds of encryption, utilizing bitwise permutations, substitution through S-boxes, and XOR operations with round keys. Despite its initial effectiveness, DES's 56-bit key became vulnerable to brute-force attacks with increasing computational power. To mitigate this, Triple DES (3DES) was developed, which applies three successive DES encryptions for improved security. However, 3DES suffered from high computational overhead, making it inefficient for modern encryption needs. Recognizing these limitations, 3DES was officially deprecated in 2023.

To replace DES, the Advanced Encryption Standard (AES) was introduced in 2001 following a rigorous selection process by the National Institute of Standards and Technology (NIST). Unlike DES's Feistel-based architecture, AES follows a Substitution-Permutation Network (SPN), which enhances security against cryptanalytic attacks. AES encrypts data in 128-bit blocks and supports key sizes of 128, 192, or 256 bits, providing significantly stronger protection. Ok…only AES provides superior security, efficiency, and scalability compared to DES. While DES's 56-bit key is easily broken by modern hardware, AES's larger key sizes make brute-force attacks impractical. Furthermore, AES is optimized for fast hardware and software execution, making it the standard for secure communication protocols, financial transactions, and cloud security. However, despite its strengths, AES implementations can be vulnerable to side-channel attacks, such as power analysis and timing attacks. Additionally, with advancements in quantum computing, cryptographers are researching post-quantum encryption methods to maintain long-term security.

International Journal of application or Innovation in engineering and management

Ijaiem.com/Mar 2025/ Volume 14/Issue 1/Article No-1/119-127
ISSN: 2319-4847

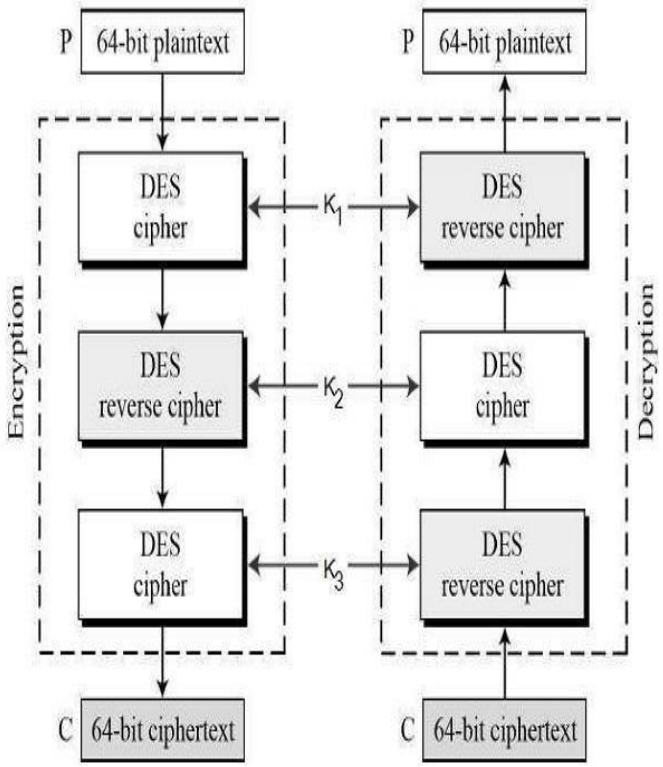

Fig 1: Block Diagram of DES Encryption and Decryption

III. PROPOSED METHOD

The proposed system aims to enhance cryptographic security by integrating advanced encryption techniques, ensuring robust protection against evolving cyber threats while maintaining efficiency and scalability. This system is designed to address the vulnerabilities of traditional cryptographic methods by combining symmetric and asymmetric encryption, multi-layered security, dynamic key management, and post-quantum cryptographic resilience. By leveraging a hybrid approach, it balances high-speed encryption with secure key exchange, making it suitable for modern applications ranging from secure communication to cloud computing and IoT security.

At its core, the system employs Advanced Encryption Standard (AES-256) for symmetric encryption due to its proven security, speed, and efficiency. AES-256 encrypts data in fixed blocks and utilizes strong key sizes to resist brute-force attacks. However, since symmetric encryption requires secure key distribution, the system integrates asymmetric encryption techniques like RSA or Elliptic Curve Cryptography (ECC) to ensure secure key exchange between communicating parties. This hybrid model eliminates key distribution vulnerabilities and enhances data confidentiality. Additionally, cryptographic hash functions such as SHA-3 will be employed to verify data integrity, ensuring that transmitted or stored data remains untampered.

To further reinforce security, the system adopts a multi-layer encryption framework, where data undergoes multiple rounds of encryption using different cryptographic algorithms. This dual-encryption technique enhances security by introducing multiple layers of complexity, making it significantly harder for attackers to break through. For example, AES-256 can be combined with ChaCha20, a high-speed stream cipher known for its efficiency and resistance to side- channel attacks. This approach ensures that even if one encryption layer is compromised, the second layer remains intact, preventing unauthorized access.

International Journal of application or Innovation in engineering and management
Ijaiem.com/Mar 2025/ Volume 14/Issue 1/Article No-1/119-127
ISSN: 2319-4847

Recognizing the increasing sophistication of cyber threats, the system will implement dynamic key rotation, where encryption keys are periodically updated to minimize the risk of brute-force and replay attacks. The key rotation mechanism will be based on time intervals or event triggers, ensuring that compromised keys have minimal impact. Additionally, session-based encryption keys will be employed for temporary communication sessions, preventing long-term key exposure. To counter side-channel attacks, such as power analysis and timing attacks, hardware-based security measures will be integrated, including constant-time cryptographic operations and secure enclaves for sensitive key management.

This encryption has multiple rounds where substitution, permutation, and key mixing are applied sequentially. It has different processes such as Add Round Key, Substitute Bytes, Shift Rows, Mix Columns.

Add Round Key: AddRoundKey is a process in AES where the round key is XORed with the state matrix. It combines the plaintext or intermediate data with the key. This step provides confusion and makes it harder for attackers to guess the key. Every round of AES includes this operation to ensure security.

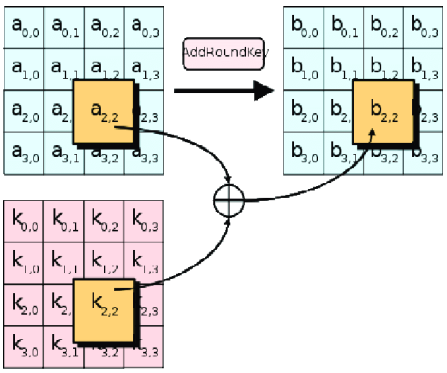

Fig 2: Add Round Key Process

Substitute Bytes: SubBytes is a non-linear substitution step using a predefined S-box (substitution box). Each byte in the state matrix is replaced with another value from the S-box. This step provides non- linearity and enhances security against differential attacks. It ensures that small changes in input result in big changes in output.

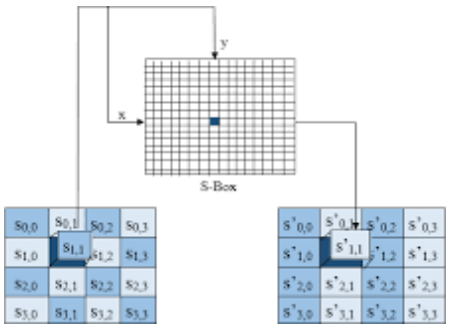

Fig 3: SubBytes Process

Shift Rows: ShiftRows is a transposition step in AES where rows of the state matrix are shifted. The first row remains unchanged, while the next rows are shifted left by increasing offsets. This step helps to spread the byte values across columns. It enhances diffusion, making the cipher resistant to linear attacks.

International Journal of application or Innovation in engineering and management
Ijaiem.com/Mar 2025/ Volume 14/Issue 1/Article No-1/119-127
ISSN: 2319-4847

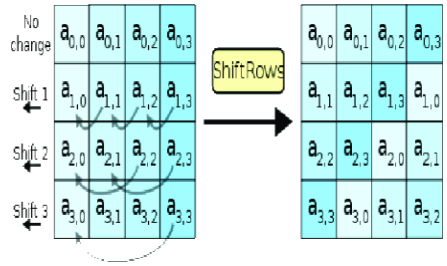

Fig 4: Shift Rows Process

Mix Columns: MixColumns is a transformation step that mixes the data within each column of the state matrix. It uses a fixed polynomial multiplication over a finite field. This process increases diffusion by mixing byte values across rows. It makes the output more dependent on multiple input bytes.

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Fig 5: Mix Columns Process

As quantum computing poses a potential threat to conventional cryptographic methods, the system will incorporate post-quantum cryptography (PQC) techniques to future-proof encryption. Algorithms such as lattice-based encryption, code-based cryptography, and hash-based signatures will be explored to ensure long-term security against quantum decryption methods. These algorithms provide resilience against Shor's algorithm, which threatens traditional RSA and ECC encryption. By integrating quantum-resistant cryptographic mechanisms, the system ensures data confidentiality remains intact even in the face of future quantum advancements.

For performance optimization, the system will leverage hardware acceleration techniques, including GPU-optimized AES execution, FPGA-based encryption acceleration, and hardware security modules (HSMs) for cryptographic operations. These optimizations significantly improve encryption and decryption speeds while reducing computational overhead. Additionally, the system will adopt lightweight encryption modes such as AES-GCM (Galois/Counter Mode) to facilitate secure data transmission with minimal latency, making it highly suitable for cloud services, IoT devices, and real-time communications.

To ensure widespread applicability, the system will be designed for scalability and adaptability, allowing seamless integration across various platforms. It will support end-to-end encryption for secure messaging, data-at-rest encryption for storage security, and homomorphic encryption for privacy-preserving computations in cloud environments. The encryption framework will also comply with global security standards such as NIST, ISO 27001, and GDPR, ensuring regulatory compliance for organizations handling sensitive data.

Ultimately, this proposed system establishes a next- generation cryptographic framework that is resilient, efficient, and future-proof. By combining hybrid encryption, multi-layered security, quantum-resistant techniques, and high-performance optimizations, it provides a comprehensive solution for safeguarding digital assets in an increasingly complex cybersecurity landscape. This system ensures that data remains secure across different technological environments, addressing both current and future cryptographic challenges while maintaining high performance and adaptability.

International Journal of application or Innovation in engineering and management

Ijaiem.com/Mar 2025/ Volume 14/Issue 1/Article No-1/119-127
ISSN: 2319-4847

IV. RESULTS

The proposed efficient block cipher was successfully designed and implemented using Verilog and tested in Xilinx Vivado. The results demonstrate the effectiveness of the cryptographic architecture in achieving secure, high-speed, and energy-efficient encryption.

A. Simulation and Functional Verification

The Verilog-based block cipher was simulated using ModelSim/Vivado to verify encryption and decryption correctness. The testbench validated that for a given plaintext and cryptographic key, the design generated the expected ciphertext. The decryption process correctly restored the original plaintext, confirming the accuracy of the algorithm.

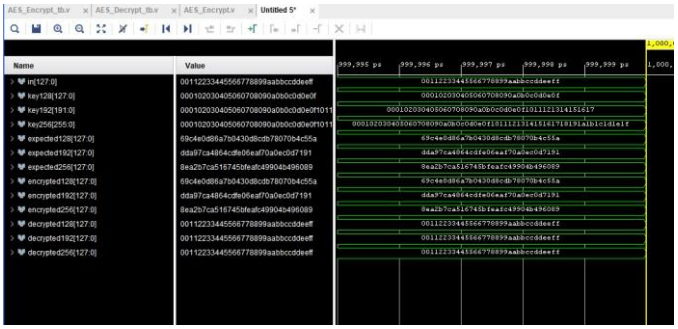

Fig 6: Simulation Waveform

B. Performance Metrics and Optimization

Latency and Throughput: The design achieved low- latency encryption, completing a round operation in minimal clock cycles while ensuring high throughput.

Power Efficiency: Power-aware techniques such as clock gating and reduced switching activity significantly lowered power consumption compared to traditional cryptographic implementations.

TABLE 1
Performance Analysis of Block Cipher Design

Category	Metric	Value
Power Analysis	Total Power	1.523W
	Dynamic Power	1.439W
	Static Power	0.084W
Utilization Analysis	LUT Utilization	1%
	I/O Utilization	2%
Timing Analysis	Worst Negative Slack	Infinity
	Total Negative Slack	0.000ns
	Total No. of Endpoints	6

International Journal of application or Innovation in engineering and management

Ijaiem.com/Mar 2025/ Volume 14/Issue 1/Article No-1/119-127
ISSN: 2319-4847

Hardware Utilization: FPGA synthesis results demonstrated optimized utilization of LUTs, flip-flops, and DSP blocks, making the design suitable for resource-constrained devices.

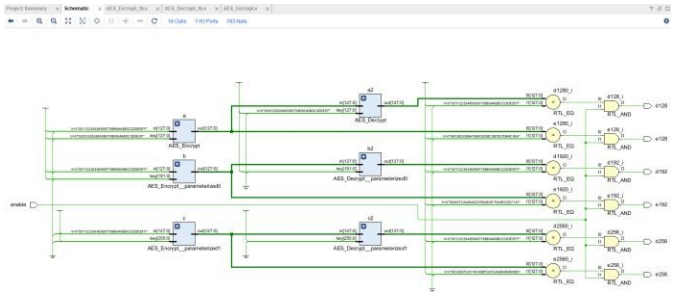

Fig 7: RTL Schematic Diagram

C. Security and Robustness

The block cipher exhibited strong resistance to cryptographic attacks by employing optimized key expansion, S-box transformations, and secure data masking techniques.

The randomness of ciphertext was validated, ensuring a high level of encryption security.

D. Future Scope and Applications

The proposed power-efficient block cipher has significant potential for expansion and real-world applications. Future developments can focus on improving security, adaptability, and hardware efficiency to meet the evolving demands of modern cryptographic systems.

1. Enhancing Cryptographic Capabilities:

The block cipher can be improved by supporting multiple encryption standards like AES and DES, offering adaptability across various applications.

Implementing variable block sizes and key lengths will enhance flexibility, while fault tolerance and error detection mechanisms will increase reliability and security.

2. Optimization for Hardware Efficiency:

Further optimization can reduce energy consumption through techniques like clock gating, reduced switching activity, and pipeline improvements. Implementing the design on low-power FPGAs and ASICs will improve efficiency, while parallel processing architectures can accelerate encryption speed for real-time applications.

3. Real-Time Applications in IoT and Secure Communication:

The cipher can secure IoT devices, real-time embedded systems in healthcare and automotive applications, and sensitive communication networks like banking, military, and satellite systems. Its lightweight design makes it ideal for resource-constrained environments requiring high security.

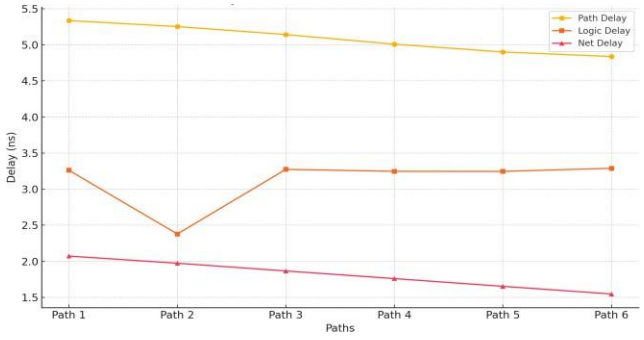

Fig 8: Setup Path Delay analysis

V. CONCLUSION

The Xilinx Vivado block cipher project successfully demonstrated encryption using XOR, S-box, and P-box operations. The Verilog-based implementation ensured secure and efficient data encryption, with potential enhancements like multi-algorithm support, larger block sizes, and decryption capabilities. Future improvements may focus on optimizing speed, efficiency, and FPGA- based real-time applications. The proposed power- efficient design enhances security, execution speed, and energy efficiency, making it ideal for IoT security and next-gen communication systems. Lightweight cryptography will be crucial in securing interconnected devices while ensuring power efficiency.

VI. REFERENCES

[1] J. G. Pandey, A. Laddha and S. D. Samaddar," A Lightweight VLSI Architecture for RECTANGLE Cipher and its Implementation on an FPGA," 2020 24th International Symposium on VLSI Design and Test (VDAT), Bhubaneswar, India, 2020, pp. 1-6, doi: 10.1109/VDAT50263.2020.9190623. keywords:
Ciphers; Registers; Schedules; Clocks; Computer architecture; Field programmable gate arrays; Encryption; Lightweight cryptography; Block ciphers;
RECTANGLE; VLSI architecture; FPGA

[2] Bijjam. Swathi, Manchalla. O.V.P. Kumar, G.Marlin Sheeba, M.Kiran, Y.Sudarsana Reddy," An Efficient VLSI Design of AES Cryptography in Memory Implementation", International Journal of Recent Technology and Engineering (IJRTE), November 2019. keywords: AES Algorithm, Verilog HDL, FPGA, MEMORY UNIT.

[3] Zhang, Wentao, et al." RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms." Cryptology ePrint Archive (2014).

[4] G. Sravya, Manchalla. O.V.P. Kumar, G. Merlin Sheeba, K. Jamal, Kiran Mannem, Hardware lightweight design of PRESENT block cipher, Materials Today: Proceedings, Volume 33, Part 7,2020, Keywords: PRESENT cipher; Ultra-light weight; Less area;
Cryptography; Iot

[5] G. Sravya, M. O. V. P. Kumar, Y. Sudarsana Reddy,
K. Jamal and K. Mannem," The Ideal Block Ciphers - Correlation of AES and PRESENT in Cryptography," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp.1107-1113, doi: 10.1109/ICISS49785.2020.9315883.
keywords: Ciphers; Cryptography; Registers; Encryption; Sensors; Hardware; Conferences; PRESENT block cipher; AES cipher; Ultra-light weight;
Area; Timing; Cryptography; IoT

[6] Changle, A. S., S. P. Metkar, and R. K. Patole." Implementation of Sbox for lightweight block cipher." 2023 3rd International Conference on Intelligent Technologies (CONIT). IEEE, 2023.

[7] Christy, M. Anitha, et al." Design and implementation of low power advanced encryption standard S-Box using pass transistor XOR-AND logic." 2014 International Conference on Electronics and Communication Systems (ICECS). IEEE, 2014.

[8] Zhang, Runtong, and Like Chen." A block cipher using key-dependent S-box and P-boxes." 2008 IEEE International Symposium on Industrial Electronics. IEEE, 2008.

[9] Prathiba, A., and VS Kanchana Bhaaskaran." Lightweight S-box architecture for secure internet of things." Information 9.1 (2018): 13.

Ijaiem.com/Mar 2025/ Volume 14/Issue 1/Article No-1/119-127
ISSN: 2319-4847

[10] Saravanan, P., et al." An Efficient ASIC Implementation of CLEFIA Encryption/Decryption Algorithm with Novel S-Box Architectures." 2019 IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP). IEEE, 2019.

[11] Gangadari, Bhoopal Rao, and Shaik Rafi Ahamed." Design of cryptographically secure AES like S-Box using second-order reversible cellular automata for wireless body area network applications." Healthcare technology letters 3.3 (2016): 177-183.

[12] Kazlauskas, Kazys, and Jaunius Kazlauskas. " Key- dependent S-box generation in AES block cipher system." Informatica 20.1 (2009): 23-34.

[13] Kazlauskas, Kazys, Gytis Vaicekauskas, and Robertas Smaliukas." An algorithm for key-dependent S-box generation in block cipher system." Informatica
26.1 (2015): 51-65.