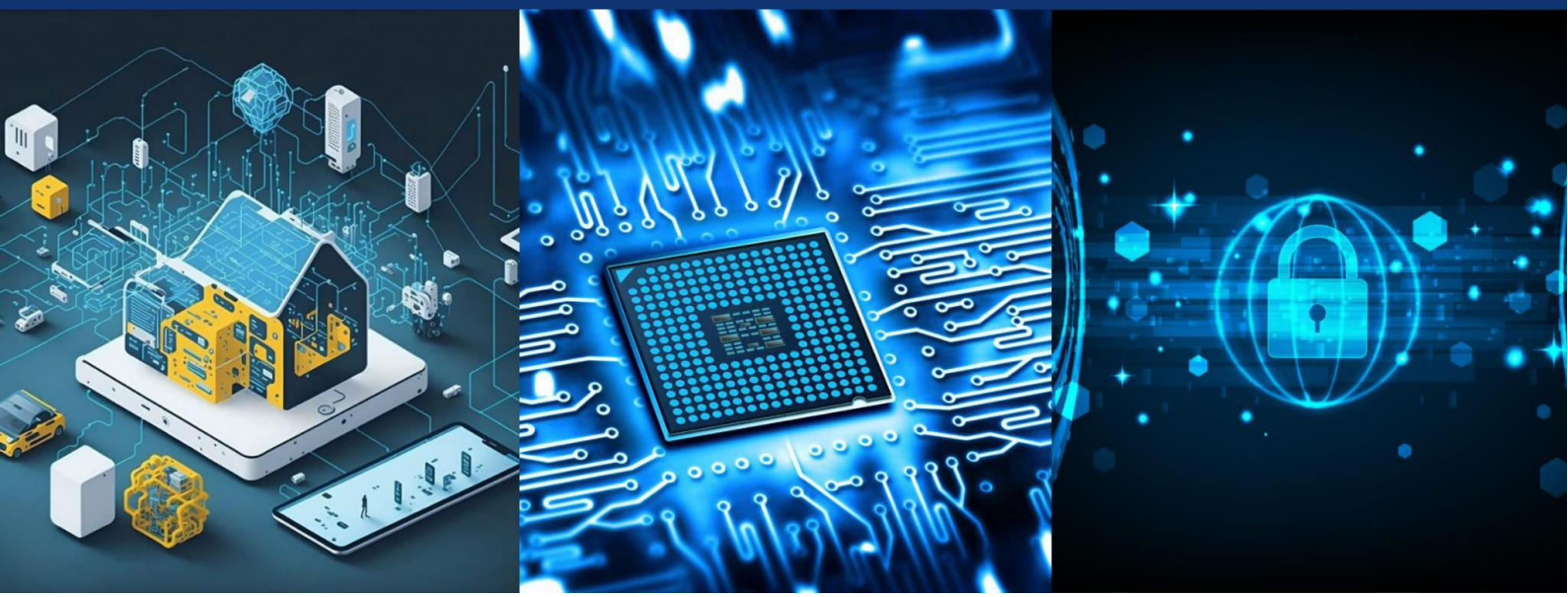
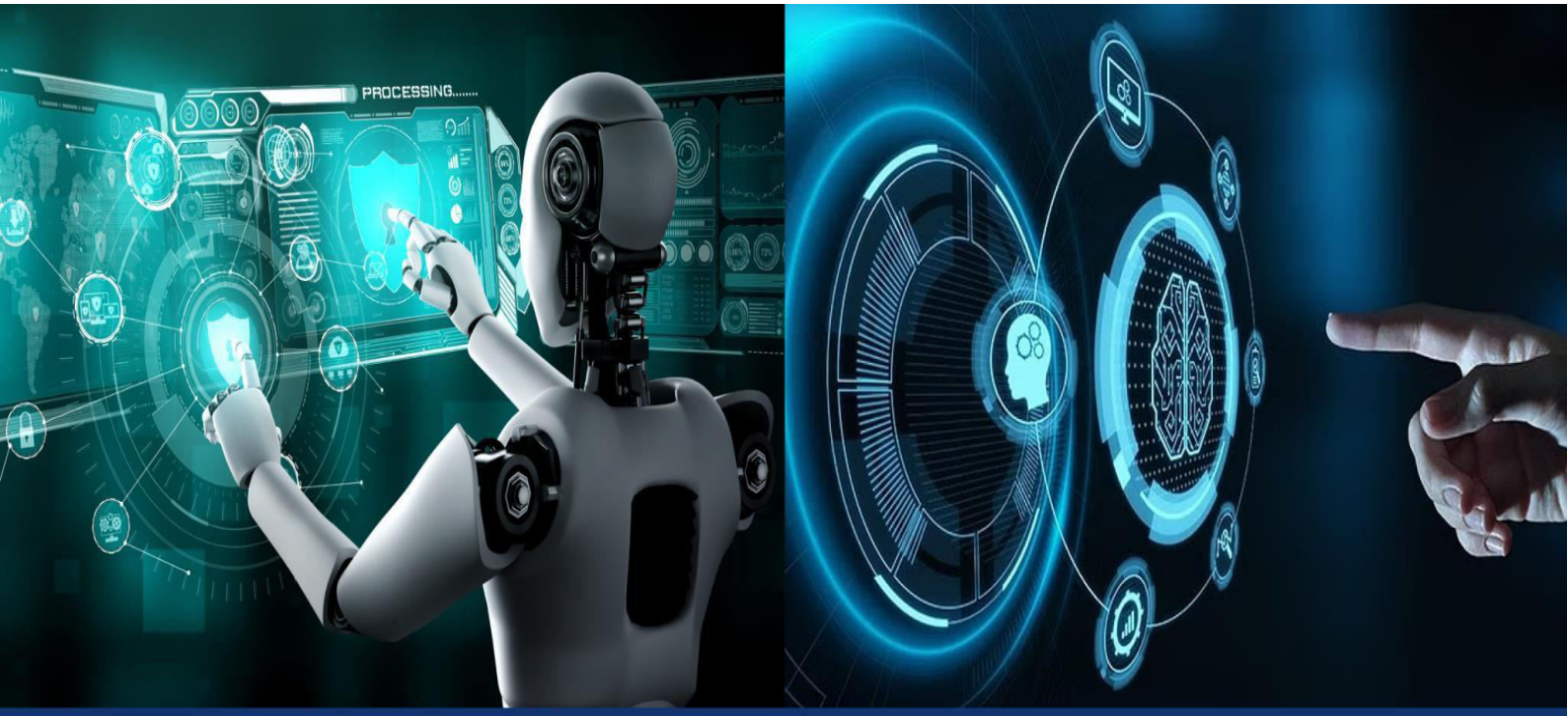
ISSN(O): 2320-9801
ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771 **Volume 14, Issue 4, April 2026**

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404114

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Design of a 128-Bit Advanced Encryption Standard and Optimization of the S-Box

V. Adinarayana, D Sri Purva, P Danisha Nagasai, G S R Padmavathi,T Harsha Vardhan

Associate Professor, Dept. of E.C.E, Gayatri Vidya Parishad College for Degree and PG Courses (A), Visakhapatnam, Andhra Pradesh, India

B. Tech Students, Dept. of E.C.E, Gayatri Vidya Parishad College for Degree and PG Courses (A), Visakhapatnam, Andhra Pradesh, India

ABSTRACT: The Advanced Encryption Standard (AES) is a widely adopted symmetric key cryptographic algorithm used for securing data in modern communication systems due to its robustness and efficiency. This work presents an optimized implementation of AES-128, focusing on both encryption and decryption architectures. In the proposed design, the conventional lookup table (LUT)-based Substitution Box (S-Box) is replaced with a Galois Field (GF) arithmetic-based S-Box, where substitution is performed using multiplicative inversion in GF(2^8) followed by an affine transformation. This approach significantly reduces memory requirements and enhances hardware efficiency by eliminating the need for large precomputed tables.

Furthermore, an optimized decryption architecture is developed to ensure correct inverse transformations while minimizing latency and resource utilization. Experimental results demonstrate improved area utilization and reduced hardware complexity without compromising performance. The design is suitable for VLSI and embedded security applications.

KEYWORDS: AES-128, Galois Field, S-Box, VLSI, Cryptography, FPGA, Hardware Optimization

I. INTRODUCTION

The rapid growth of digital communication has increased the demand for secure cryptographic systems. AES is one of the most reliable symmetric encryption algorithms due to its strong security and efficiency. AES operates on 128-bit blocks and supports key sizes of 128, 192, and 256 bits.

Among these, AES-128 is widely used in hardware implementations due to its balance between performance and complexity. The algorithm consists of Sub Bytes, Shift Rows, Mix Columns, and Add Round Key transformations.

Traditional implementations use LUT-based S-Boxes, which consume significant memory. To overcome this limitation, this work proposes a Galois Field (GF)-based S-Box, improving hardware efficiency and reducing area. Additionally, an optimized decryption architecture is introduced.

II. RELATED WORK

In [1] authors discussed the design principles of substitution boxes (S-Boxes) emphasizing nonlinearity and resistance to cryptographic attacks such as linear and differential cryptanalysis. Their work laid the foundation for secure S-Box construction, which is a critical component in AES. The study highlights that strong S-Box design significantly enhances overall encryption robustness.

In [2] a comprehensive tutorial on linear and differential cryptanalysis was presented, explaining how weaknesses in substitution and permutation structures can be exploited. The authors showed that the effectiveness of AES largely depends on the strength of its nonlinear components, particularly the S-Box, which must exhibit high confusion and avalanche properties.

In [3] the original design of the Rijndael algorithm (AES) was introduced, where the SubBytes operation is implemented using a lookup table (LUT)-based S-Box. Although this approach ensures fast execution, it requires

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

considerable memory resources, making it less efficient for hardware-constrained environments such as embedded and VLSI systems.

In [4] authors provided a survey on hardware security challenges, focusing on trade-offs between area, power, and performance in cryptographic implementations. The study emphasized the importance of optimizing key components such as S-Boxes to achieve efficient hardware designs without compromising security.

In [5] optimized implementations of lightweight cryptographic S-Boxes were proposed using advanced techniques such as SAT solvers. The results demonstrated significant improvements in area efficiency and performance, indicating the potential for alternative S-Box realization methods beyond traditional LUT-based designs.

In [6] a compact AES S-Box design based on Galois Field (GF) arithmetic was introduced. The authors demonstrated that multiplicative inversion in GF(2^8), combined with affine transformation, can replace LUT-based implementations, resulting in reduced hardware complexity and lower area consumption. In [7] an efficient GF(2^8) inversion circuit was proposed using redundant arithmetic techniques. This approach significantly reduced computational complexity and improved performance, making it suitable for high-speed cryptographic hardware implementations.

In [8] researchers presented an area-optimized combined S-Box and inverse S-Box design. Their work focused on minimizing hardware resources while maintaining functionality, which is particularly beneficial for FPGA and ASIC implementations.

Overall, existing works indicate that while LUT-based S-Boxes provide high speed, they suffer from high memory usage. In contrast, GF-based and composite field arithmetic techniques offer a promising alternative by reducing area and power consumption while maintaining strong cryptographic properties. However, achieving an optimal balance between speed and hardware efficiency remains a key challenge, which motivates the proposed hybrid approach in this work.

III. PROPOSED ALGORITHM

A. AES Encryption

- AES-128 performs 10 rounds of transformations:
- **Sub Bytes:** Nonlinear substitution using GF(2^8) inversion + affine transformation
- **Shift Rows:** Row-wise cyclic shifting
- **Mix Columns:** Column-wise mixing using polynomial multiplication
- **Add Round Key:** XOR with round key

The proposed design replaces LUT S-Box with **GF-based computation**, reducing memory usage.

B. Galois Field S-Box

The transformation is defined as:

$$S(x) = A \cdot x^{-1} \oplus b$$

where:

- x^{-1}: multiplicative inverse in GF(2^8)
- A: affine matrix
- b: constant vector

The irreducible polynomial used is:

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

This design improves efficiency while maintaining strong cryptographic properties.

C. Decryption Architecture

Two approaches:

- GF-based inverse S-Box

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404114

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- LUT-based inverse S-Box

IV. HARDWARE IMPLEMENTATION

A. Modules

- AES Encryption Core
- AES Decryption Core
- GF-based S-Box
- LUT-based Inverse S-Box

B. Simulation Setup

- Plaintext: 00112233445566778899AABBCCDDEEFF
- Key: 000102030405060708090A0B0C0D0E0F
- Ciphertext: 69C4E0D86A7B0430D8CDB78070B4C55A
- Simulation performed using Vivado

V. SIMULATION RESULTS

The simulation of the proposed AES design is carried out using Xilinx Vivado 2018.2. Functional verification is performed for both encryption and decryption modules using standard AES-128 test vectors (FIPS-197).

The encryption module successfully converts the plaintext 00112233445566778899aabbccddeeff into the ciphertext 69c4e0d86a7b0430d8cdb78070b4c55a. Similarly, the decryption module correctly retrieves the original plaintext from the ciphertext using the same key.

Simulation waveforms confirm that the outputs match the expected results, indicating correct implementation of Sub Bytes, Shift Rows, Mix Columns, and Add RoundKey operations. The results show PASS for both encryption and decryption test cases.

The proposed design demonstrates correct functionality with efficient hardware utilization. It ensures reliable data transformation with accurate key expansion and round operations. Overall, the implementation achieves successful validation of AES algorithm behavior in terms of correctness and performance.

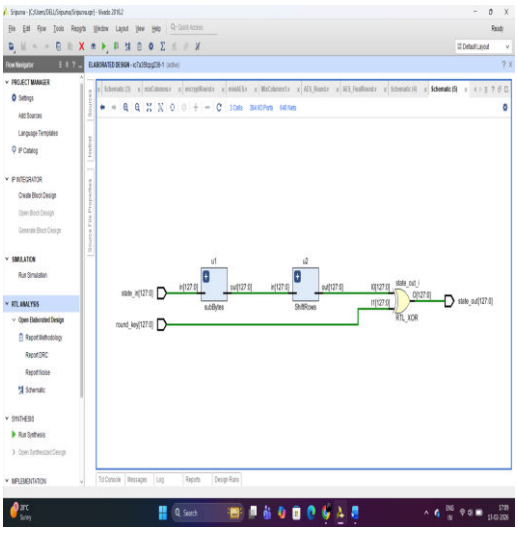


Fig.1. final round

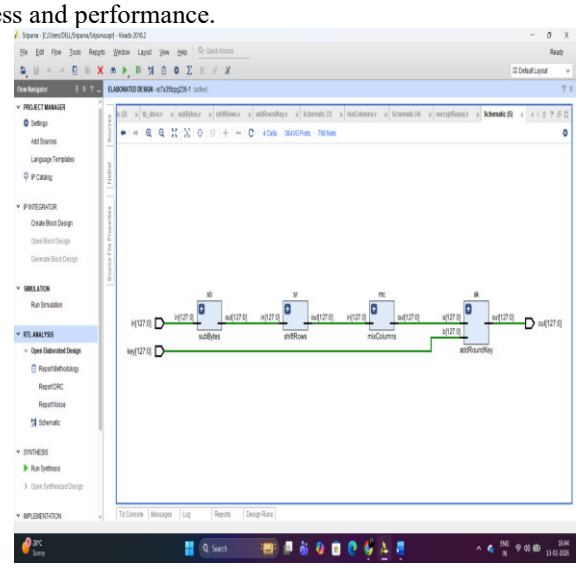


Fig. 2. Encryption round

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404114

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

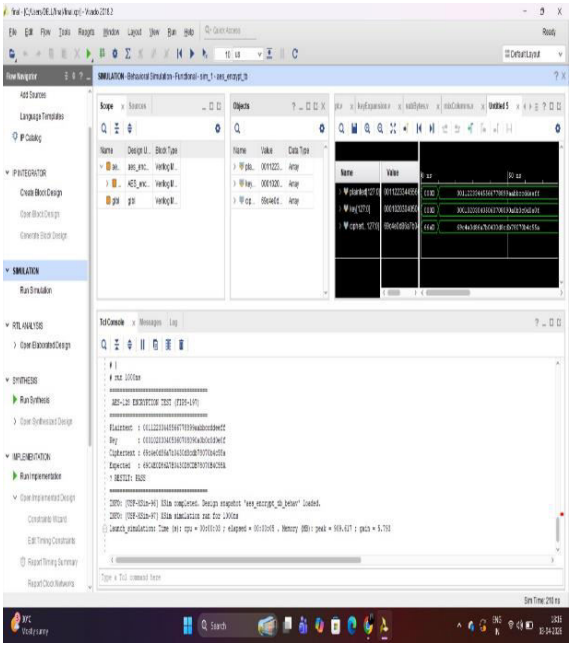


Fig.3.Encrypted stimulation

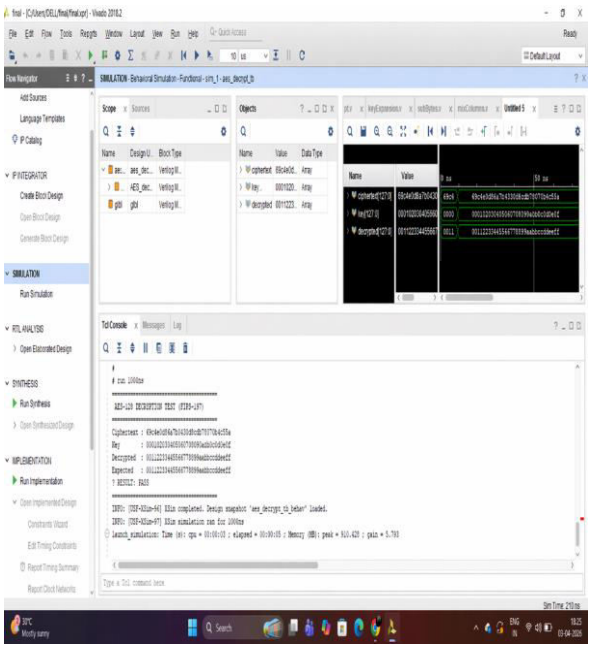


Fig 4. Decryption of the plain text

VI. CONCLUSION AND FUTURE WORK

The simulation results show that the proposed AES design is successfully implemented and verified using standard test vectors. The encryption and decryption modules produce correct outputs, confirming the proper functionality of all AES operations. The design ensures accurate data transformation with reliable performance.

The proposed implementation provides an efficient hardware realization of the AES algorithm with correct key expansion and round processing. In future, the design can be further optimized in terms of area, power consumption, and speed. Additionally, the performance can be analyzed on different FPGA platforms and compared with other optimized AES architectures.

REFERENCES

1. A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Advances in Cryptology (CRYPTO)*, Springer, 1986, pp. 523–534.
2. H. M. Heys, "A tutorial on linear and differential cryptanalysis," *Cryptologia*, vol. 26, no. 3, pp. 189–221, 2002.
3. J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*, Springer, 2002.
4. S. Akter, K. Khalil, and M. Bayoumi, "A survey on hardware security: Current trends and challenges," *IEEE Access*, vol. 11, pp. 77543–77565, 2023.
5. J. Feng, Y. Wei, F. Zhang, E. Pasalic, and Y. Zhou, "Novel optimized implementations of lightweight cryptographic S-boxes via SAT solvers," *IEEE Trans. Circuits Syst. I*, vol. 71, pp. 334–347, 2024.
6. D. Canright, "A very compact S-box for AES," in *CHES 2005*, Springer, 2005, pp. 441–455.
7. R. Ueno, N. Homma, Y. Sugawara, Y. Nogami, and T. Aoki, "Highly efficient GF(2^8) inversion circuit based on redundant GF arithmetic and its application to AES design," in *CHES 2015*, Springer, vol. 9293, pp. 63–80.
8. A. Reyhani-Masoleh, M. Taha, and D. Ashmawy, "New area record for the AES combined S-box/inverse S-box," in *IEEE ARITH*, 2018, pp. 145–152.
9. G. Kim, H. Kim, Y. Heo, Y. Jeon, and J. Kim, "Generating cryptographic S-boxes using reinforcement learning," *IEEE Access*, vol. 9, pp. 83092–83104, 2021.
10. J. Chen, Z. Gong, Y. Tang, and X. Dong, "A comprehensive analysis of lightweight 8-bit S-boxes," *J. Information Security and Applications*, vol. 70, 2022.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

11. S. T. J. Fenn, M. Benaissa, and D. Taylor, "GF(2^m) multiplication and division over the dual basis," *IEEE Trans. Computers*, vol. 45, no. 3, pp. 319–327, 1996.
12. A. Ibrahim and F. Gebali, "Compact finite field multiplication processor for cryptographic IoT devices," *Sensors*, vol. 22, no. 2090, 2022.
13. B. Rashidi, "Lightweight 8-bit S-box and combined S-box/S-box^{-1}," *Int. J. Circuit Theory Appl.*, vol. 49, pp. 2348–2362, 2021.
14. T. Shah and A. Qureshi, "S-box on subgroup of Galois field," *Cryptography*, vol. 3, 2019.
15. A. Manzoor, A. H. Zahid, and M. T. Hassan, "A new dynamic substitution box using chaotic maps," *IEEE Access*, vol. 10, pp. 74164–74174, 2022.
16. NIST, "Advanced Encryption Standard (AES)," FIPS PUB 197. [17] J. Daemen and V. Rijmen, "AES Proposal: Rijndael." [18] Canright, "A Very Compact AES S-Box," IEEE.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details