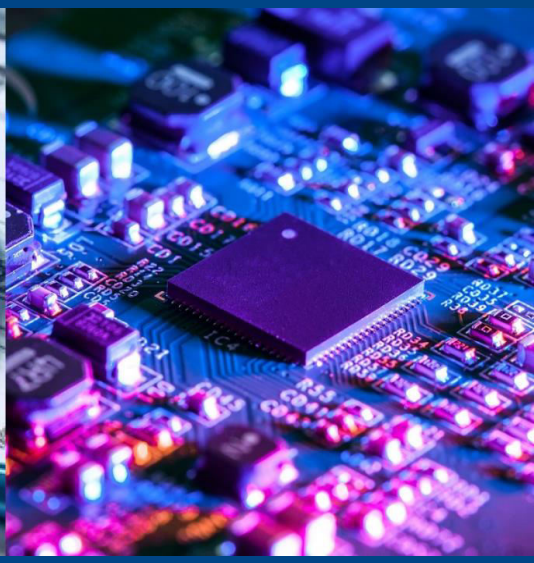
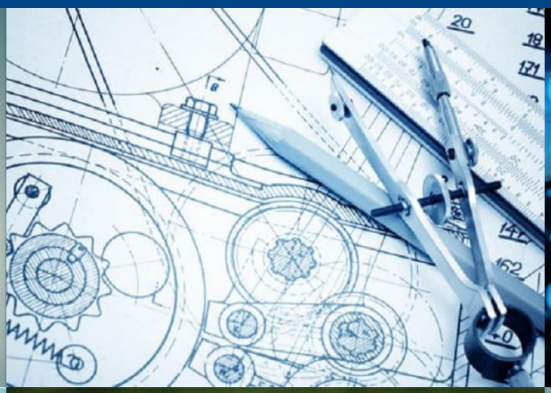
ISSN: 2582-7219

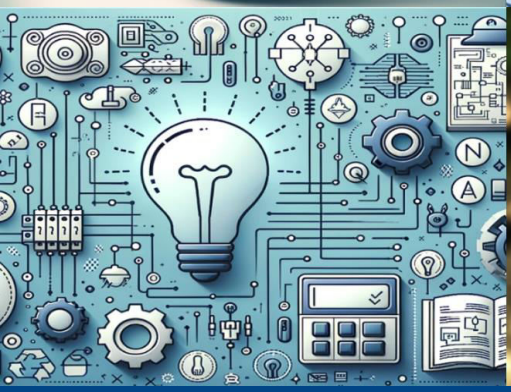




International Journal of Multidisciplinary Research in Science, Engineering and Technology

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



Impact Factor: 8.206 **Volume 9, Issue 3, March 2026**

© 2026 IJMRSET | Volume 9, Issue 3, March 2026| DOI: 10.15680/IJMRSET.2026.0903225

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

AES S-Box Hardware with Efficiency Improvement Based on LMO

M.N.S.Greeshma[1], M.Charan[2], D.Sowjanya[3], Dr.K.Murali Babu[4]

U.G. Student, Department of ECE, SVIET Engineering College, Nandamuru, Pedana, Andhra Pradesh, India[1,2,3]

Professor, Department of ECE, SVIET Engineering College, Nandamuru, Pedana, Andhra Pradesh, India[4]

ABSTRACT: This project presents an efficient hardware implementation of the AES S-Box using composite field arithmetic and linear mapping optimization. The Advanced Encryption Standard (AES) is widely used for secure data encryption, where the S-Box plays a critical role in determining performance. In this system, composite field representation is used instead of direct lookup tables to reduce hardware complexity and power consumption. The proposed design uses optimized linear transformations and Galois Field arithmetic to improve area-time efficiency. By applying multiplicative and exponential offset techniques, the performance of the S-Box is significantly enhanced.

The system supports both encryption and decryption operations and achieves better efficiency compared to conventional designsThis implementation is suitable for applications requiring high-speed and secure cryptographic operations such as embedded systems and communication devices.

KEYWORDS: AES, S-Box, Galois Field, Encryption, Decryption, Hardware Optimization.

I. INTRODUCTION

The Advanced Encryption Standard (AES) is a widely used cryptographic algorithm for securing digital data. It is commonly used in applications such as banking, communication systems, and data protection. One of the most important components of AES is the S-Box (Substitution Box), which performs substitution operations to provide security against attacks. The efficiency of AES largely depends on how the S-Box is implemented. There are two main methods to implement the S-Box: Direct lookup table and Composite field arithmetic. In this project, composite field arithmetic is used because it reduces hardware complexity and power consumption.

.

II. RELATED WORK

Many researchers have proposed different methods to implement the AES S-Box with improved performance and efficiency. In early designs, the S-Box was implemented using lookup tables (LUTs), where all input-output values are stored in memory. This method provides fast computation but requires large memory and higher power consumption, making it less suitable for hardware-constrained systems.To overcome these limitations, researchers introduced composite field arithmetic techniques. In this method, the original Galois Field GF(2^8) is converted into smaller subfields such as GF((2^4)^2) or GF(((2^2)^2)^2). This reduces the complexity of the inversion operation, which is the main function of the S-Box. As a result, hardware area and power consumption are significantly reduced.

Several works have focused on optimizing the inversion circuit using algorithms like the Itoh–Tsujii method. This approach improves efficiency by simplifying the multiplicative inverse operation in Galois Fields. Researchers have also explored different basis representations, such as polynomial basis and normal basis, to further improve performance.In addition, many studies proposed optimization of linear transformations, including isomorphic mapping and affine transformation. These transformations are implemented using XOR operations, and their efficiency depends on the structure of transformation matrices. Reducing the number of XOR gates helps in minimizing hardware area and delay.

Recent advancements include the use of multiplicative and exponential offset techniques to expand the design space and find better optimized S-Box structures. These methods improve the area-time (AT) efficiency by reducing both delay and hardware complexity. Some designs also support both encryption and decryption operations, making them

© 2026 IJMRSET | Volume 9, Issue 3, March 2026| DOI: 10.15680/IJMRSET.2026.0903225

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

more flexible for real-world applications.Despite these improvements, achieving a balance between low area, high speed, and low power consumption remains a major challenge. Therefore, further optimization techniques are still being explored to enhance AES S-Box performance.

III. METHODOLOGY

Here we are considering the image encryption. This new method of image encryption is based on a linear feedback shift register(LFSR). In order to encrypt the given plain image we need to make use of the linear feedback shift register , which generates the random numbers used in the encryption process. Since we use the random number generator , the attacker cannot guess the next number in the sequence, even if he/she have some idea about some numbers in the generated sequence. This method proposes a new technique to encrypt the color image using LFSR to generate random numbers used in the reorder position of the image pixels. The method is divided in to two stages , namely, encryption and decryption. In the encryption stage uses two phases of encryption. First phase involved in the encryption stage is the row level encryption and the second phase is the column level encryption. Finally we need to apply the XOR operation to complete the encryption stage . Since we use the XOR operation we need to convert the image into a binary format before encryption. So that we can perform a smooth encryption process. To decode or decrypt the image we need to do the reverse operation of encryption.

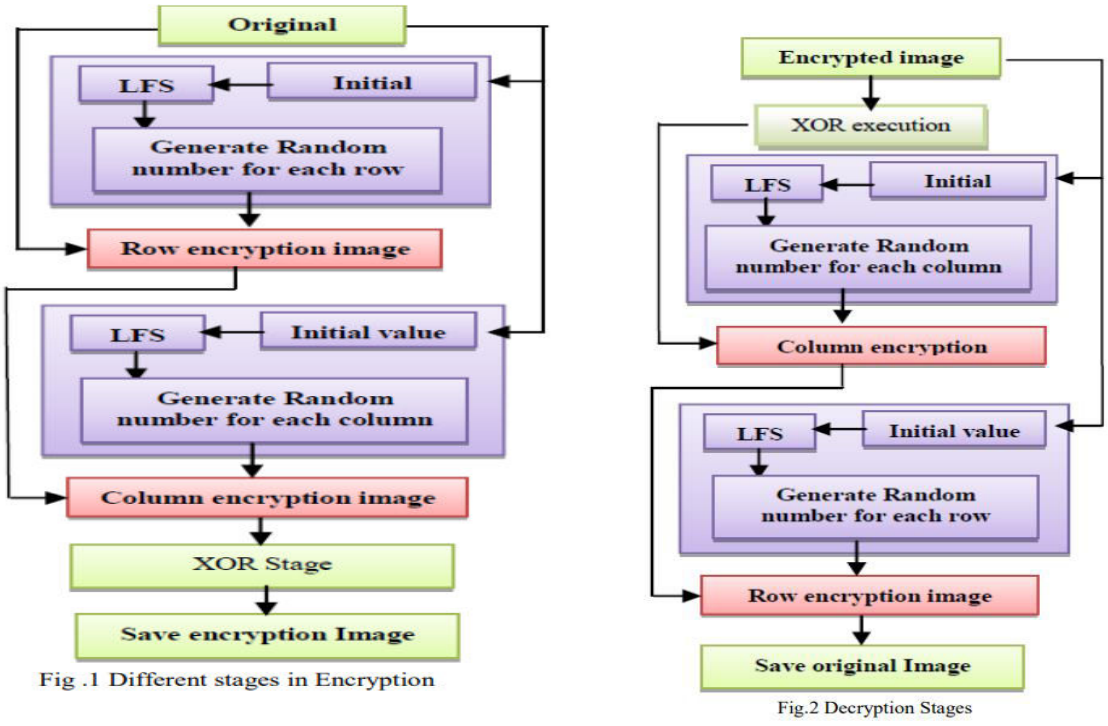


Fig .1 Different stages in Encryption

Fig.2 Decryption Stages

FIG 1: BLOCK DIAGRAM OF ENCRYPTION AND DECRYPTION PROCESS

This diagram shows a simple process of image encryption. First, random numbers are generated for each row of the image to encrypt it. Then, random numbers are generated for each column to further encrypt the image. Finally, an XOR operation is applied, which combines the encrypted rows and columns to produce the final secure encrypted image.Encryption ensures that the original image cannot be easily understood. Random numbers add unpredictability, making the process more secure. The XOR stage acts like a final lock, giving strong protection to the image data.This diagram explains the process of image decryption. It starts with the encrypted image, then applies an XOR operation to reverse the final lock. Next, random numbers are generated for each column using LFS, and column decryption is performed. After that, random numbers are generated for each row, and row decryption is carried out. Finally, the original image is reconstructed and saved. In simple terms, the decryption process carefully undoes each encryption step—XOR, column, and row operations—to recover the original image securely.

© 2026 IJMRSET | Volume 9, Issue 3, March 2026| DOI: 10.15680/IJMRSET.2026.0903225

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

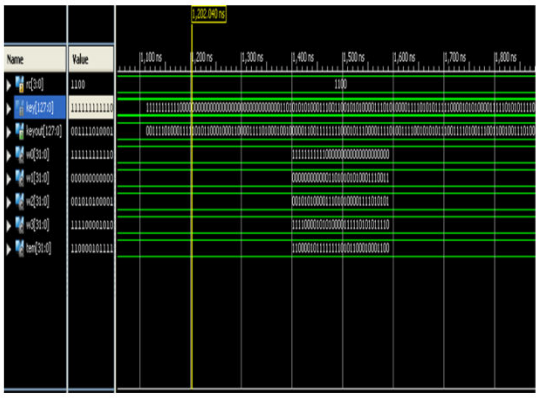
International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

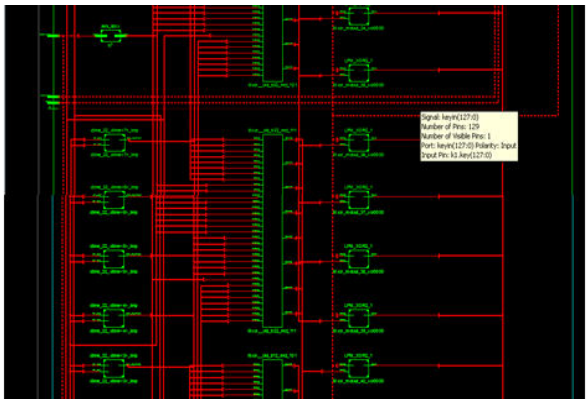
IV.EXPERIMENTAL RESULTS

The proposed AES S-Box design was implemented and analyzed to evaluate its performance in terms of area, delay, and efficiency. The results show that the composite field based implementation requires less hardware compared to traditional lookup table methods. The use of optimized linear mapping reduces the number of XOR operations, which helps in minimizing circuit complexity.The design achieves lower delay due to efficient inversion using Galois Field arithmetic. Both encryption and decryption operations are supported with improved performance. The area-time (AT) product is significantly reduced, indicating better overall efficiency. Simulation results confirm that the proposed system provides faster computation and lower power consumption. Overall, the system performs better than conventional S-Box implementations.

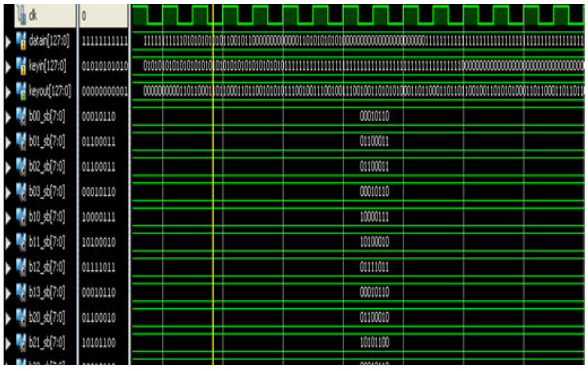
FIG 2:



(a) Simulation for keyexpansion

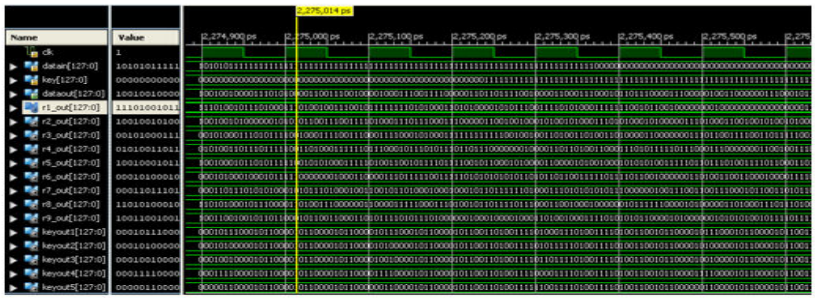


(b) Elaborated Design



(c) Simulation for rounds

(d)Simulation for AES S-Box



(e)Simulation for AES

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Fig 2:shows the results of IoT Based weather monitoring station using raspberry pi (a) Simulation for keyexpansion,(b) Elaborated Design of AES after simulation ,(c)Simulation for Rounding program,(d) Simulation for AES S-Box(e) Simulation results for AES Program

V. CONCLUSION

The result shows that the design with the pipelining technology and special data transmission mode can optimizethe chip area effectively. Meanwhile, this design reduces power consumption to some extent, for the power consumption is directly related to the chip area.Therefore the encryption device implemented in this method can meet some practical applications. As the S-box is implemented by look-up-table in this design, the chip area and power can still be optimized. So the future work should focus on the implementation mode of S-box. Mathematics in Galois field (28) can accomplish the bytes substitution of the AES algorithm, which could be another idea of further research.

In this paper, the most widely used public-key cryptography, RSA cryptography, has been introduced. The Chinese Remainder Theorem (CRT) and the CRT-based RSA cryptosystem have been described. Then, the attacks, especially the implementation attacks to the CRT-based RSA cryptosystems have been reviewed. Some countermeasures to the implementation attacks were also presented.

REFERENCES

[1]J.Yang,J.Ding, N.Li and Y.X.Guo,“FPGA-based design and implementation of reduced AES algorithm” IEEE Inter.Conf. Chal EnvirSci Com Engin (CESCE), Vol.02, Issue.5-6, pp.67-70, Jun 2010.
[2]A.M.Deshpande, M.S.Deshpande and D.N.Kayatanavar,“FPGAImplementation of AES Encryption and Decryption”IEEEInter.Conf.Cont,Auto,Com,and Ener., vol.01,issue04, pp.1-6,Jun.2009.
[3] Hiremath.S. and Suma.M.S.,“Advanced Encryption StandardImplemented on FPGA” IEEE Inter.Conf. Comp Elec Engin.(IECEE),vol.02,issue.28,pp.656-660,Dec.2009.
[4]Abdel-hafeez.S.,Sawalmeh.A. and Bataineh.S.,“High Performance AESDesign using Pipelining Structure over GF(28)” IEEE Inter Conf.SignalProc and Com.,vol.24-27, pp.716-719,Nov. 2007.
[5] Rizk.M.R.M. and Morsy, M., “Optimized Area and Optimized SpeedHardware Implementations of AES on FPGA”, IEEE Inter Conf. Desig Tes Wor.,vol.1,issue.16,pp.207-217, Dec. 2007.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com