A LIGHTWEIGHT IMAGE ENCRYPTION ALGORITHM BASED ON SECURE KEY GENERATION

Sk.Syed Afreed[1], V.Venky[2], M.Tarakeswar[3], P.Phani Kumar[4]

[1] Student, Electronics and Communication Engineering, VVIT, Andhra Pradesh, India
[2] Student, Electronics and Communication Engineering, VVIT, Andhra Pradesh, India
[3] Student, Electronics and Communication Engineering, VVIT, Andhra Pradesh, India
[4] Student, Electronics and Communication Engineering, VVIT, Andhra Pradesh, India

ABSTRACT

This Cryptography deals with the security and integrity of the data. Initially many algorithms were developed to encode and decode the data but for securing large and confidential data, the existing algorithms are not reliable, so AES was developed as a new standard for encrypting and decrypting data. Initially it is mainly used to protect highly confidential data, later many applications in networking began using AES as a standard to protect their data. It is primarily used to protect sensitive data, though it is also applied to network backends to enhance data security. AES employs blocks that are 16 bytes long, and its keys can range in size from 128 bits to 256 bits. The main purpose of using Verilog instead of standard VHDL is that it provides very less operation time and the propagation delay to encode and decode the data are comparatively less than other HDL languages. Before AES, DES was used as the encryption standard. The main drawback of DES is that the fixed key size of 56 bits. This problem is solved by AES by providing the flexibility of using required variable key size.

Keywords— *Advanced Encryption Standard, Input text, Cipher text, Verilog.*

1. INTRODUCTION

The Advanced Encryption Standard (AES) is a symmetric key block cipher published by NIST in 2001, which encrypts 128-bit data blocks using key lengths of 128, 192, or 256 bits, with 10, 12, or 14 rounds of processing respectively. It is part of symmetric key cryptography, where the same key is used for both encryption and decryption, offering faster and more efficient security compared to asymmetric encryption. Cryptography ensures data confidentiality, authentication, and integrity, and includes methods like AES, the Data Encryption Standard (DES), and modern stream ciphers. AES relies on substitution-boxes (S-boxes) to create confusion and enhance security. Dynamic S-boxes, key-dependent and used in algorithms like Blowfish, offer better cryptographic strength compared to static ones. Encryption protocols like Pretty Good Privacy (PGP), S/MIME, and SSL/TLS ensure secure communication over various platforms by employing a combination of encryption algorithms.

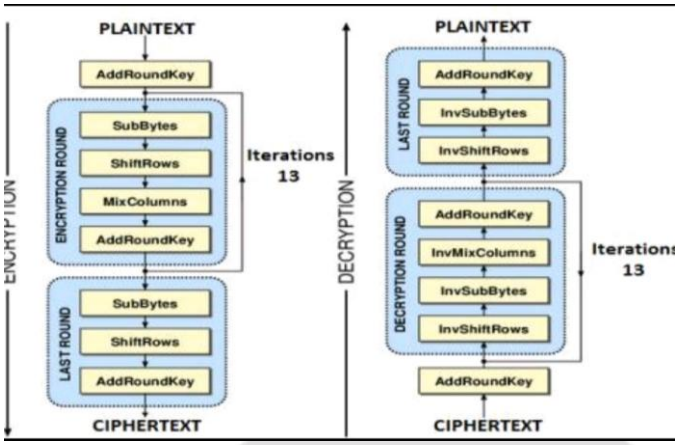

Fig -1: Architecture of 256 AES Algorithm

.2. LITERATURE SURVEY

[1]M. Rajeswara Rao, Dr.R.K.Sharma, SVE Department, NIT Kurushetra "FPGA Implementation of combined S box and Inv S box of AES" 2017 4th International conference on signal processing and integrated networks (SPIN)",This paper proposes a combined architecture for the AES S-Box and inverse S-Box (Inv S-Box) using composite field arithmetic in GF(2^8), reducing hardware complexity compared to the traditional LUT-based approach. By sharing the multiplicative inverse module, the design significantly reduces gate count, area, and power consumption.

[2] Nalini C. Iyer ; Deepa ; P.V. Anandmohan ; D.V. Poornaiah "Mix/InvMixColumn decomposition and resource sharing in AES". This paper presents compact architectures for the AES MixColumn and inverse MixColumn transformations to reduce area cost in hardware implementations. By utilizing byte and bit-level decomposition, the design optimizes resource sharing and rearranges output terms for FPGA architecture, reducing reconfigurable logic area by 40% and critical path delay by 9%.

[3] Yulin Zhang ; Xinggang Wang; "Pipelined implementation of AES encryption based on FPGA" 2010 IEEE International Conference on Information Theory and Information Security.''This paper presents an outer-round pipelined architecture for AES-128 encryption on FPGA, utilizing Block RAM to store S-box values and combining operations within a single round to reduce critical delay. Hardware-based implementations, using optimizations like pipelining and lookup tables, significantly improve throughput and key generation time, addressing the growing need for high-speed cryptographic algorithms.

[4] C. Sivakumar ; A. Velmurugan ; "High Speed VLSI Design CCMP AES Cipher for WLAN (IEEE 802.11i)" 2007 International Conference on Signal Processing, Communications and Networking. ''This paper proposes a high-speed, non-pipelined FPGA implementation of the AES-CCMP cipher for wireless LAN, utilizing Xilinx development tools and Virtex-It Pro FPGAs. The AES-CCMP core operates at 194/148 MHz, achieving a throughput of 2.257 Gbps for encryption and 1.722 Gbps for decryption. Compared to software implementations, this hardware solution offers enhanced security and faster encryption speeds. The paper highlights the advantages of AES-CCMP over the insecure WEP algorithm, making it a suitable choice for securing wireless LAN environments.

3.1 EXISTING METHOD:

The Data Encryption Standard (DES), developed by IBM in the early 1970s, is a symmetric-key cryptographic method that uses the same private key for both encryption and decryption. Despite its relatively short 56-bit key, DES was widely used in applications such as VPNs, email encryption, and electronic payments. However, as computational power increased, DES became vulnerable to brute-force attacks, leading to the development of Triple DES, which enhances security by applying DES three times with different keys, resulting in a 168-bit key length. While DES is still used in some legacy systems, it is generally discouraged, especially after the National Institute of Standards and Technology (NIST) disapproved its use in government applications since 2005. Today, Advanced

Encryption Standard (AES) is preferred due to its larger key sizes (128, 192, or 256 bits), 128-bit block size, and more complex encryption method using substitution-permutation networks, making it more secure and efficient than DES, which uses a Feistel network and 64-bit block size. AES operates on a 4x4 state matrix and performs multiple rounds (10, 12, or 14 based on the key length) involving sub-bytes, shift rows, mix columns, and round key addition. Each round uses a unique key generated through key expansion, with the number of 32-bit words in the key denoted as Nk (4, 6, or 8), and the number of rounds (Nr) corresponding to 10, 12, or 14 respectively. AES ensures high security by transforming plaintext into ciphertext that cannot be decrypted without the appropriate key, making it the modern standard in symmetric encryption

Table -1: Information

parameter	DES	AES
Key length	56 bits	128 bits
Block length	64 bits	128 bits
Rounds	16	10

Table -2: AES Bits for Existing Method

AES Bits	Key Length (Nk)	Block length (Nb)	No of Rounds (Nr)
128bit	4	4	10
192bit	6	4	12
256bit	8	4	14

3.2 PROPOSED METHOD

In the AES algorithm, the input block, output block, and state array each consist of 128 bits, organized as four 32-bit words, denoted by Nb = 4. The key length determines the number of 32-bit words in the key, represented by Nk, which can be 4, 6, or 8 for key sizes of 128, 192, or 256 bits, respectively. The number of rounds (Nr) in AES depends on Nk: 10 rounds for Nk = 4, 12 for Nk = 6, and 14 for Nk = 8. Each round involves four core operations—SubBytes, ShiftRows, MixColumns, and AddRoundKey. These rounds rely on unique round keys generated from the original key through the key expansion process. For a 128-bit key, 10 unique round keys are generated. The input plaintext is first converted into hexadecimal and organized into a 4x4 state matrix, on which all transformations are applied. After completing all rounds, the final matrix is converted back into text. In the proposed design pipeline structure, each color represents a different round (e.g., Mix-round 0 to Mix-round 14). Each 32-bit word undergoes a mix operation per round. For instance, in cycle 1, word 0 undergoes a mix operation denoted as cycle1 [round0 (mix_0)].

Table -1: AES Bits for Proposed Method

AES Bits	Key Length (Nk)	Block length (Nb)	No of Rounds (Nr)
128bit	4	4	10
192bit	6	4	12
256bit	8	4	14

Table -2: SBox Information

S box	Shift	Mix	Cycle
		Mix_0	1
Sub_0	-	Mix_1	2
Sub_1	Shift_0	Mix_2	3
Sub_2	Shift_1	Mix_3	4
Sub_3	Shift_2	-	5
Key_7	Shift_3	Mix_0	6
Sub_0	-	Mix_1	7
Sub_1	Shift_0	Mix_2	8
Sub_2	Shift_1	Mix_3	9
Sub_3	Shift_2	-	10
Key_3	Shift_3	Mix_0	11
Sub_0	-	Mix_1	12
Sub_1	Shift_0	Mix_2	13
Sub_2	Shift_1	Mix_3	14
Sub_3	Shift_2	-	15
-	Shift_3	Mix_0	16
.	.	Mix_1	17
Key_11	.	Mix_2	18
Sub_0	-	Mix_3	19
Sub_1	Shift_0	.	.
Sub_2	Shift_1	.	.
Sub_3	Shift_2	-	.
-	Shift_3	Mix_0	71
		Mix_1	72
		Mix_2	73
		Mix_3	74

4. RESULTS

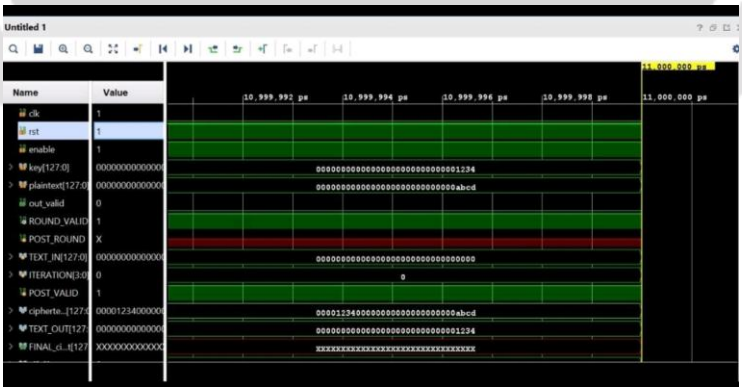

Fig -1:

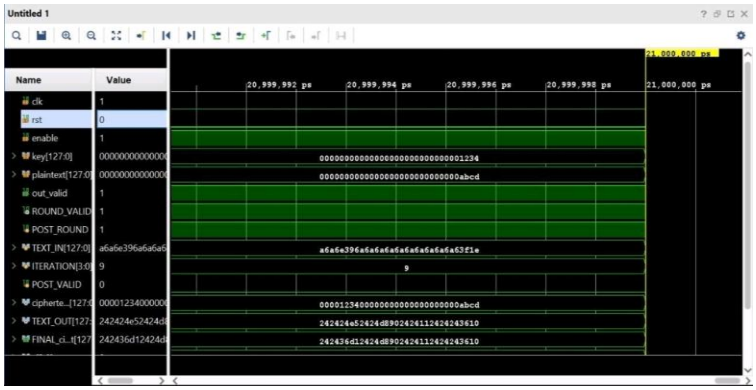

Fig -2:

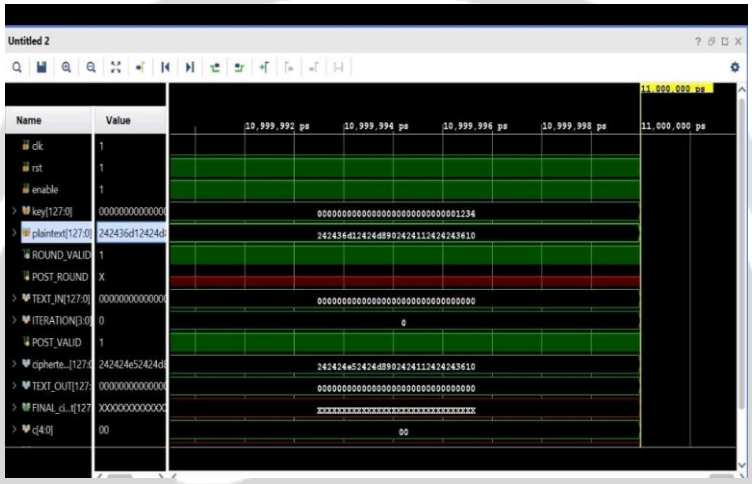

Fig -3:

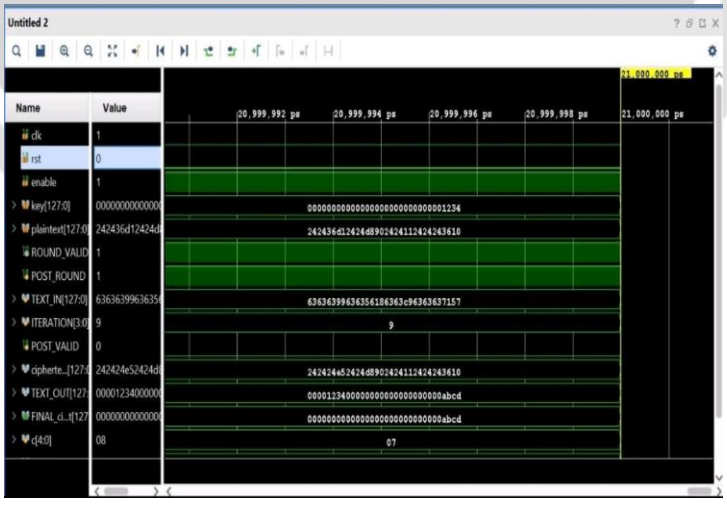

Fig -4:

Fig -4

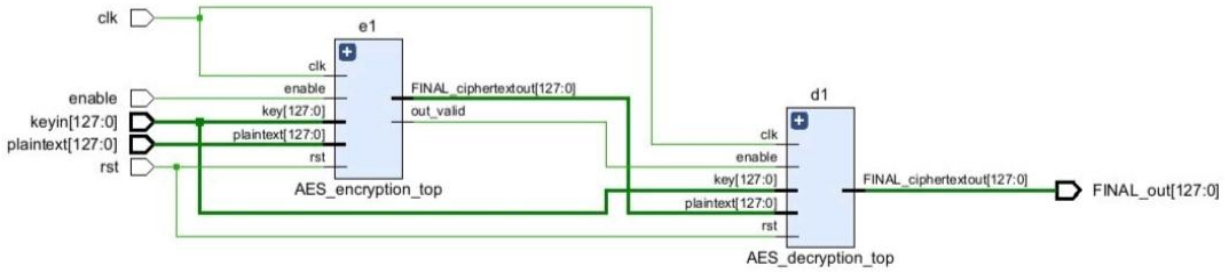

Fig -5: RTL Schemetic Image

Power estimation from Synthesized netlist. Activity derived from constraints files, simulation files or vectorless analysis. Note: these early estimates can change after implementation.

Total On-Chip Power:	**205.461 W (Junction temp exceeded!)**
Design Power Budget:	**Not Specified**
Power Budget Margin:	**N/A**
Junction Temperature:	**125.0°C**
Thermal Margin:	-324.1°C (-172.2 W)
Effective ϑJA:	1.9°C/W
Power supplied to off-chip devices:	0 W
Confidence level:	Low

Fig -6: Power

5. CONCLUSION

The proposed AES design is implemented using Verilog to optimize clock cycle usage and reduce average operation time for both encryption and decryption. Compared to VHDL, Verilog demonstrates better performance, requiring fewer clock cycles and resulting in lower power consumption. AES is inherently more secure than DES due to its longer key sizes and additional round operations. While DES uses only a 56-bit key, AES supports key sizes of 128, 192, and 256 bits, offering significantly stronger protection. Implementing AES in hardware using System Verilog further enhances adaptability and is ideal for high-speed real-time applications due to its improved efficiency and flexibility.

6. REFERENCES

[1] Jamal, K., Chari, K. M., & Srihari, P. (2019). Test pattern generation using thermometer code counter in TPC technique for BIST implementation. Microprocessors and Microsystems, 71, 102890.

[2] Shady Mohamed Soliman, Baher Magdy and Mohamed A. AbdE1 Ghany, “Efficient implementation of the AES algorithm for security applications”, IEEE 2016.

[3] J. Daemen and V. Rijmen, The block cipher Rijndael, Smart Card research and Applications, LNCS 1820, Springer-Verlag, pp. 288-296.

[4] Jamal, K., Srihari, P., & Kanakasri, G. (2016). Test Vector Generation using Genetic Algorithm for Fault Tolerant Systems. International Journal of Control Theory and Applications (IJCTA), 9(12), 5591-5598.

[5] Kumar, A., & Gupta, R. (2016). Design and implementation of AES algorithm in Verilog. International Journal of Engineering Research and Technology, 5(4), 217-220.

[6] J. Orlin Grabbe, "The DES algorithm illustrated.

[7]Zabina Kouser, Manish Singhal, and Amit M.Joshi, "FPGA implementation of Advanced encryption standard algorithm", IEEE international conference on Recent advances and innovations in Engineering, (ICRAIE-2016).

[8] Jamal, K., Srihari, P., Chari, K. M., & Sabitha, B. (2018). Low power test pattern generation using test-per-scan technique for BIST implementation. ARPN Journal of Engineering and Applied Sciences.

[9] Mohini Mohurle and Vishal V. Panchbhai, "Review on realization of AES encryption and decryption with power and area optimization",1st IEEE Conference on power electronics, intelligent control and energy system (ICPEICES-2016).

[10] Yehya A. Nasser, Mohammad A. Bazzoun, Samih Abdul Nabi, "AES algorithm implementation for a simple low cost portable 8- bit microcontroller", IEEE 2016.