An Efficient Encryption Encoder Using Permutation with Advanced Encryption Standard (AES) in Verilog

Ranajay Kar[1], Dr.A.Ch.Sudhir[2]

[1]*M.Tech, Dept. of ECE, GIT, GITAM (Deemed to be University), Visakhapatnam, Andhra Pradesh, India*

[2]*Assistant Professor, Dept. of ECE, GIT, GITAM (Deemed to be University), Visakhapatnam, Andhra Pradesh, India*

Abstract

Data or information security is defined as providing adequate digital confidentiality protocols specifically to shield unapproved access towards digital databases. Encryption is a method of encoding data in the form of numbers, words, and images using mathematical algorithms so that, the data becomes undecipherable to unwanted spectators.With the course of time the methods ofencryption have been upgraded and modified to meet the advanced technology needs. Now a days, the Advanced Encryption Standard (AES) has been the encryption algorithm of the sublime standard and globally recognized.

The current work focuses on designing of an Efficient Encryption Encoder using Keyed Permutation with AES for 128 bit Keys in terms of reduced delay as compared to the existing AES algorithms. All the codes have been written using Xilinx ISE Design Suite 14.7 software and the coding language is in Verilog. We have shown a comparative delay analysis between the existing algorithms and with the Keyed Permutation technique for a better understanding.

Keywords: *Data Encryption, AES, Permutation, Encryption Algorithm, Information Security, Cryptography.*

1. Introduction

Exchange of information has been the backbone of any kind of communication systems. But, not all information has always been meant for everyone out there. Sharing specific information and that too maintaining privacy and secrecy to avoid any kind of unauthorized access is quite challenging and a matter of supreme importance as far as the sensitivity of the transiting data are concerned. The history of cryptography is born along with the art of exchanging thoughts and ideas in written form. With the growing civilizations due to various social issues human beings start communicating secretly.

As a result, continuous evolution incryptography came into picture to secure the confidential information from all possible threats.

1.1 Basic Terminology of Cryptography

Cryptography is the way toward changing comprehensible and unmistakable information into tremendous information so as to verify the privacy.The first information that we have to stow away, is called plaintext, it could be in any type of these sorts, for example, characters, numerical qualities, executable projects, pictures, or data of any kind.

The data that will be imparted is called cipher text, it's an expression alludes to the series of "futile" information, or vague content that no one must comprehend, with the exception of the beneficiaries. The information will be transmitted precisely through system, numerous calculations are utilized to change plaintext into cipher text.

Cipher can be defined as a set of calculations which is utilized to change plaintext to cipher text, this technique is called encryption, and at the end of the day, it's an instrument of changing over intelligible and reasonable information into "good for nothing" information.

The Key is a contribution to the encryption calculation, and this esteem must be free of the plaintext, this information is utilized to change the plaintext into cipher text, so unique keys will yield diverse cipher text.

Computer security is a nonexclusive term for a gathering of apparatuses intended to shield any information from programmers, robbery, defilement, or cataclysmic event while enabling these information to be accessible to the clients in the meantime. The case of these gadgetries is the antivirus program. Network security alludes to any action intended to ensure the ease of use, uprightness, dependability, and wellbeing of information amid their transmission on a system.

1.2 Information Encryption

Information encryption is structured with calculations to guarantee that each key is erratic and distinctive. Cryptography utilizes two sorts of keys: symmetric and asymmetric. Symmetric keys use a solitary key for both the encryption and decoding of the ciphertext. This sort of key is known as a secret key. Most cryptographic procedures utilize symmetric encryption to encode information transmissions. Symmetric encryption, otherwise called private key encryption, utilizes a similar private key for both encryption and unscrambling. The hazard in this framework is that if either party loses the key or the key is caught, the framework is broken and messages can't be traded safely.

2. AES Algorithm Summery

The most prominent and broadly received symmetric encryption calculation liable to be experienced these days is the Advanced Encryption Standard (AES). It is found to be six time quicker than triple DES. A trade for DES was required as its key size was excessively little. With expanding figuring power, it was viewed as helpless against comprehensive key pursuit assault. The highlights of AES are as per the following: Symmetric key symmetric cipher, 128-bit information, 128/192/256-bit keys, efficient and quicker than Triple-DES, Provide full determination and configuration subtleties, Compatible with C and Java.

2.1 AES Operations

AES plays out the entirety of its calculations on bytes as opposed to bits. Subsequently, AES treats the 128 bits of a plaintext hinder as 16 bytes. These 16 bytes are masterminded in four sections and four lines for preparing as a network. In contrast to DES, the quantity of rounds in AES is variable and relies upon the length of the key. AES utilizes 10 rounds for 128-bit keys, 12 rounds for 192-bitkeys and 14 rounds for 256-bit keys. Every one of these rounds utilizes an alternate 128-bit round key, which is determined from the first AES key.

2.2AES Encryption

A run of the mill round of AES encryption has been appeared. Each round comprises of four sub-forms. The first round procedure is depicted beneath:

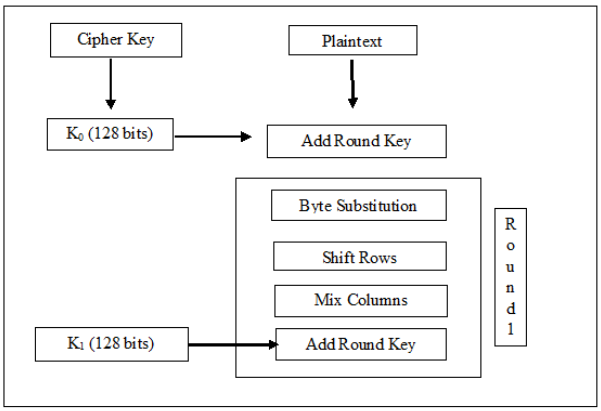

Figure 1. Encryption Rounds in AES

2.2.1 Bytes Substitution: The 16 input bytes are substituted by looking up a fixed table (S-box) given in plan. The outcome is in a lattice of four lines and four segments.

2.2.2 Rows Shifting: Every element of the four lines of the matrix is moved to the left side. Any elements that 'tumble off' are re-embedded on the right side of row. Move is completed as pursues:There is no shift in the first row. The second row is moving one position (byte) to the left. Two positions are moved to the left in the third row. Three positions are moved to the left in the fourth row. The result is a new matrix made up of the same 16 bytes but shifted from each other.

2.2.3 Blend Column Segments: Every section of four bytes is presently changed utilizing an uncommon scientific capacity. This capacity takes as information the four bytes of one section and yields four totally new bytes, which supplant the first segment. The outcome is another new grid comprising of 16 new bytes. It ought to be noticed that this progression isn't performed in the last round.

2.2.4 Add Round Key: The grid consisting of 16 bytes are presently considered as 128 bits and are XORed to the 128 bits of the round key. On the off chance that this is the last round, at that point the yield is the cipher text. Something else, the subsequent 128 bits are translated as 16 bytes and we start another comparative round.

3. Keyed Permutation in AES

A replacement box (S-box) replaces a little square of info bits with another square of yield bits. The process of substitution must be coordinated. A safe S-box will have the property that transforming one info bit will change about portion of the yield bits by and large, displaying what is known as the torrential slide impact for example it has the feature that each yield bit will rely upon each information loaded as input.

A permutation box (P-box) is a stage of the considerable number of bits: it takes the yields of all the S-boxes of one round, changes the bits, and feeds them into the S-boxes of the following round. A decent P-box has the property that the yield bits of any S-box are circulated to whatever number S-box contributions as could be expected under the circumstances. At every round, the round key (got from the key with some basic activities, for example, utilizing S-boxes and P-boxes) is consolidated utilizing some gathering task, normally XOR. Decoding is finished by essentially turning around the procedure.

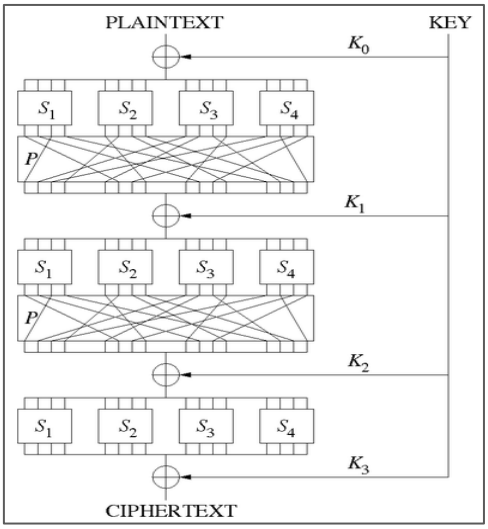

Figure 2.Substitution Permutation Network (SPN) with 3 rounds, scrambling a plain text square of 16 bits into a cipher text square of 16 bits.

4. Simulation Results

4.1 RTL Schematic (Synthesis)

In Keyed Permutation, here four input keys of 16 bytes KEYA, KEYB, KEYC, and KEYD are taken respectively with the PLAINTEXT of equal length. The output will be the CIPHERTEXT after the process of encryption is done.

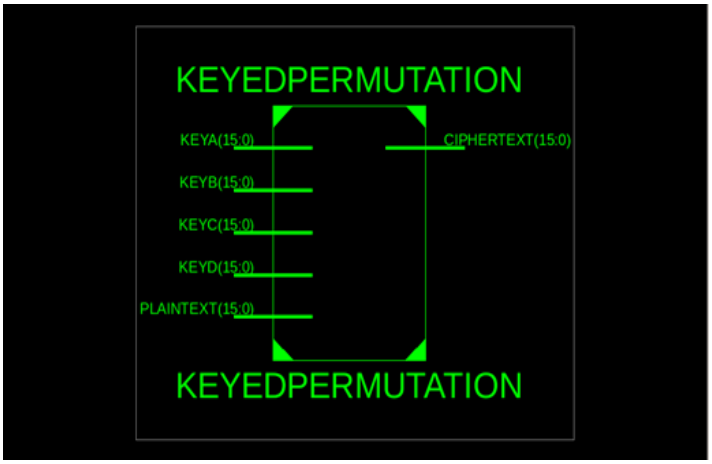

Figure 3. RTL Schematic for Keyed Permutation

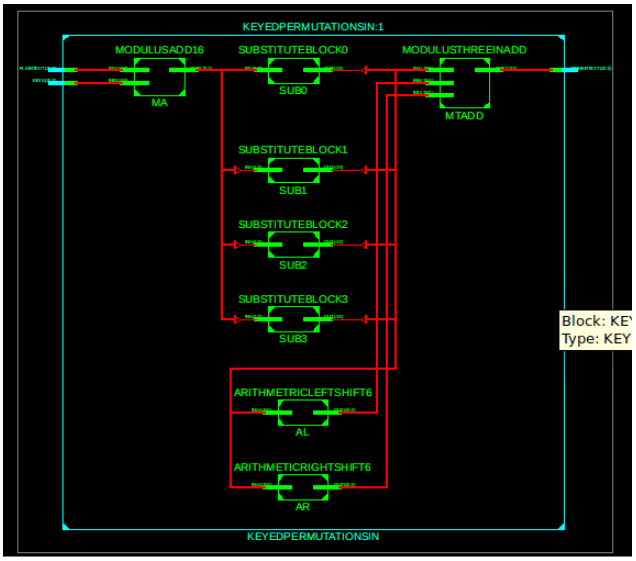

Figure 4. RTL Schematic for Top Module

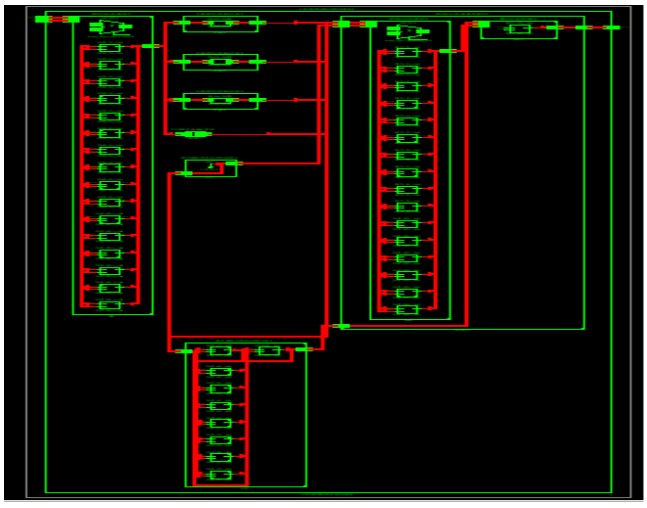

Figure 5. Technology Schematic for Top Module

To increase the efficiency of the Encryption Encoder a Symmetric Encryption technique has been used in the form of Keyed Permutation, where the Keys can be taken at random without any proper Sequence resulting in more data security.In the conventional encryption techniques basically the 128 bit Keys are taken at a single instance but, in case of Keyed Permutation 4 Keys of 16 bytes have been applied, resulting in less delay and less memory usage.

4.2Encrypted Output

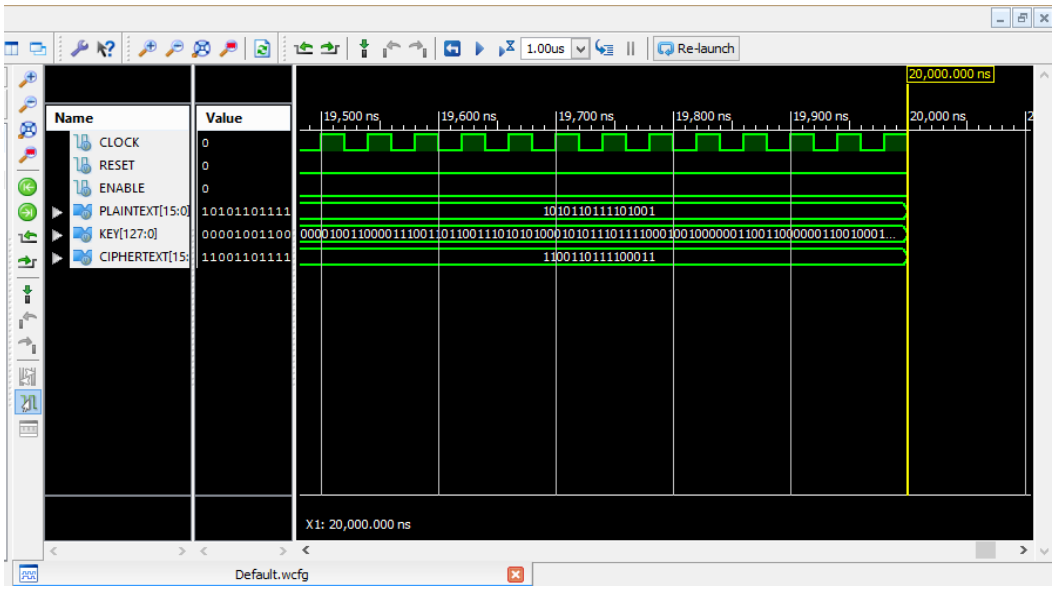

Figure 6. Simulation Result of Top module

4.3Comparative Delay analysis for AES

The Comparative Studies have been shown below:

Table 1.Delay and Memory usage for Keyed Permutation

SL. No.	Parameters	Result using Keyed Permutation Technique
1	**Delay (ns)**	16.489
2	**Total Memory Usage**	367788 kilobytes

Table 2.Comparative Delay analysis for AES

Parameter	AES algorithm Conventional (128-bit)	AES algorithm Modified (128-bit) [as per base paper]	AES algorithm using Keyed Permutation (128-bit)
Delay (ns)	54.095	39.491	16.489

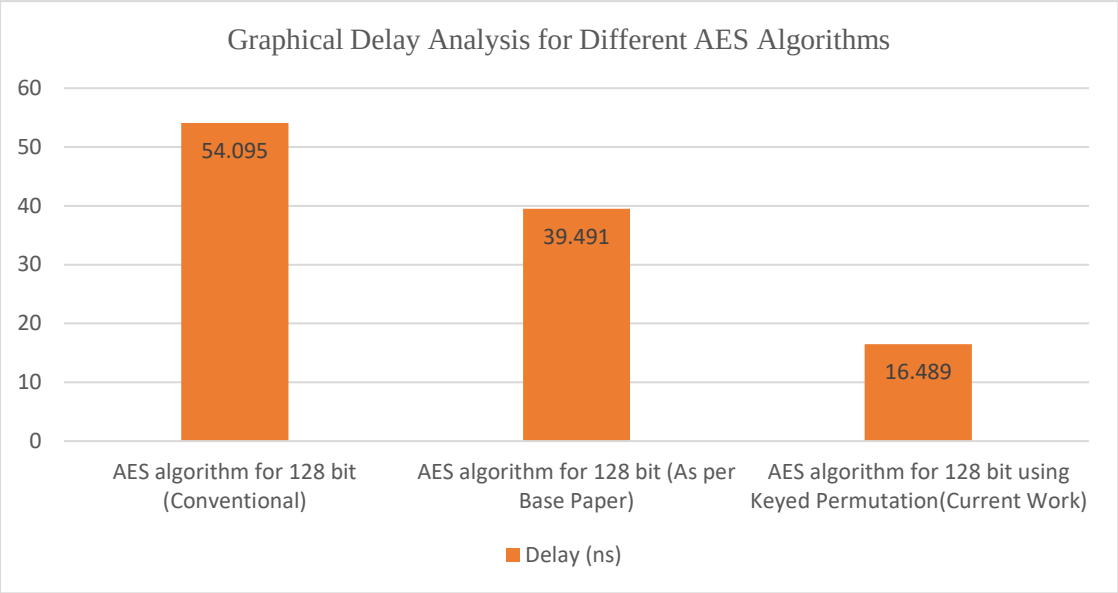

Figure 7. Graphical Delay Analysis for Different AES Algorithms

From the above results obtained we can show that while using Keyed Permutation technique the Delay has been reduced by 23.002 ns as compared to the modified methods used in the base paper.

5. Conclusion

Data Encryption is assuming the significant job in information security thus, this work accentuates on limiting the encryption time in terms of delay. In this paper the essential of AES algorithm is clarified to sum things up and the execution of its overall module in a type of shared engineering for encryption is introduced by utilizing Verilog, with the goal that the deferral or delay can be diminished.

In this work, the execution of different strategies engaged with AES have been broke down. Encryption time have been utilized to assess the cryptographic plans. The execution results demonstrate that the Advanced Encryption Standard (AES) is extremely viable as far as speed and security. The Keyed Permutation procedure has been actualized so as to lessen the delay altogether significantly.

6. References

[1] RichaKumari Sharma, S.R.Biradar and B.P.Singh, "Shared Architecture for Encryption/Decryption of AES" International Journal of Computer Applications (0975-8887) Volume 69-No.18, May 2013

[2] Jitendra Singh Chauhan and S. K. Sharma, "A Comparative Study of Cryptographic Algorithms," Int. J. Innov. Res., pp. 24–28, 2015.

[3] A. Al Hasib and A. A. M. M. Haque, "A comparative study of the performance and security issues of AES and RSA cryptography," Proc. - 3rd Int. Conf. Converg. Hybrid Inf. Technol. ICCIT 2008, vol. 2, no. November 2001, pp. 505–510, 2008.

[4] C. Narasimham and J. Pradhan, "Evaluation of Performance Characteristics of Cryptosystem Using Text Files.," J. Theor. Appl. Inf. Technol., vol. 4, no. 1, 2008.

[5] M. Mikhail, Y. Abouelseoud, and G. Elkobrosy, "Extension and Application of El-Gamal Encryption Scheme," 2014.

[6] A. Naureen, A. Akram, T. Maqsood, R. Riaz, K. H. Kim, and H. F. Ahmed, "Performance and security assessment of a PKC based key management scheme for hierarchical sensor networks," IEEE Veh. Technol. Conf., pp. 163–167, 2008.

[7] S. Farah, M. Y. Javed, A. Shamim, and T. Nawaz, "An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms," Recent advaces Inf. Sci., vol. 8, pp. 121–124, 2012.

[8] R. Tripathi and S. Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques," Int. J. Adv. Found. Res. Comput., vol. 1, no. 6, pp. 68–76, 2014.

[9] www.aiirjournal.com

[10] www.tutorialspoint.com