Appraisal of Multiple AES Modes Behavior using Traditional and Enhanced Substitution Boxes

Article · January 2020

DOI: 10.35940/ijrte.E6541.018520

5 authors, including:

Wageda Ibrahim Alsobky
Benha University
7 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Appraisal of Multiple AES Modes Behavior using Traditional and Enhanced Substitution Boxes

Medhat Mansour, Wageeda Elsobky, Ayman Hasan, Wagdy Anis

Abstract: ***The analysis of performance criteria for different cryptographic algorithms has increasingly been concerned in the last few years and that is because the majority of life applications need cryptographic algorithms to be involved in their structure to provide security for these applications such as banking services, e-government and online applications [1]. In this paper, the analytic study is executed on the most specific popular cryptographic algorithm which is "AES" technique [2][3] in order to research the impact of utilizing different models which are named "modes" on the behavior of "AES" technique and hence increases the cryptographic strength of "AES" technique. The criteria utilized to aid in judging on the influence of modes on the behavior of "AES" technique are enciphering time, throughput and strict avalanche criteria (SAC). Such influence has been clarified and presented through providing comparative analysis among modes of operation according to previously mentioned parameters. First the analytic study is proposed utilizing the traditional substitution box formula in constructing AES technique then an enhanced version of substitution box equation is included in AES technique to provide more complex and securing substitution box in constructing AES algorithm so as to measure the impact of changing the formula of substitution box on the behavior of AES technique and its cryptographic capabilities. Finally, the results of executing the modes on the behavior of AES technique in case of utilizing the traditional s-box and the enhanced version of s-box are listed in terms of the previously mentioned criteria enciphering time, throughput and (SAC) and consequently we come up with the conclusion that SAC parameter is the only criterion that shows the impact of utilizing different modes on the behavior of AES technique but the enciphering time and throughput has no role in showing the influence of utilizing distinctive modes on the behavior of AES technique regardless of changing the substitution box equation utilized in "AES" technique.***

Index Terms-Cryptographic Algorithms; Advanced Encryption Standard (AES); Modes of Operation; Strict Avalenche Criteria (SAC).

I. INTRODUCTION

Cryptography is the science of studying how to conceal and secure the different forms of data using different techniques [4], [5].

Traditional S-box which has been presented in[6], [7] is considered as just a primitive algebraic formation thus numerous of cryptanalysts exploited the weakness of traditional S-box to attack AES algorithm.

In 2007 Affine power Affine S-box was introduced by [8].

In 2011 an enhanced version of S-box was presented by which is considered an enhancement for the traditional S-box by modifying the equation of S-box. Hence, the level of security and complexity of AES algorithm depends on structure of S-box and its cryptographic properties [9].

This S-box is the core of our work in this paper.

The related works has done as a comparison among modes of AES algorithm similar to our work are presented in [10], [11].

S-box is considered the element responsible for achieving nonlinearity in AES algorithm uniquely and there is no any other component in the structure of AES algorithm is responsible for providing this significant cryptographic characteristic.

The block ciphers perform iterative transformations based on substitutions and permutations on groups of bits with fixed length which are called blocks [12], [13].

This paper is arranged at first as a preliminary section which has been proposed in section (1). Then in subsequent sections the construction of traditional S-box with its deficiencies then the construction of improved S-box with its advantages are discussed in section (2). After that the different modes of operation used by AES algorithm are illustrated in section (3). Finally, the comparison among the modes of operation in both cases is listed, and the performance is analyzed based on the experimental analysis using both MATLAB software and FPGA hardware after that the test results and conclusions are presented in Section (4) and (5) respectively.

II.OVERVIEW ON THE S-BOX

The traditional S-box of AES is constructed from equation (1).

$$S(I) = (8F) \times (I)^{-1} + (63) \quad (1)$$

Where:

(I) ⟶ represents the input byte.

$(I)^{-1}$ ⟶ represents the multiplicative inverse of the input byte over the finite field (2^8)[14].

$S(I)$ ⟶ represents the output byte result from traditional S-box.

The traditional inverse S-box is constructed by applying equation (2).

$$(I)^{-1} = (25) \times S(I) + (05) \quad (2)$$

Then taking the multiplicative inverse of the result of the previous equation over (2^8) [14], to retrieve the input byte, which is shown in equation (3)

Revised Manuscript Received on January 15, 2020.

***** Correspondence Author

Medhat Mansour, Department of Communications, University of Ain Shams, Cairo, Egypt. Email: mhamdymansour@gmail.com

Wageeda Elsobky, Department of Mathematics, University of Banha, Cairo, Egypt. Email: wageda_ibrahim@yahoo.com

Ayman Hasan, Department of Communications, University of Banha, Cairo, Egypt. Email: ayman.hasan@yahoo.com

Wagdy Anis, Prof. Dr. in Department of Communications, University of Ain Shams, Cairo, Egypt. Email: wadyanis51@yahoo.com

$$I = \left((I)^{-1}\right)^{-1} \quad (3)$$

A. Issues with Ordinary S-box

The main problem of traditional AES S-box is its weakness of complexity and security thus, we used more securing and complex version of S-box which is called an improved AES S-box. The essence of its high security and complexity is due to combining of two operations first modifying the affine conversion to make it have the biggest possible number of terms in algebraic content then moreover adding another affine conversion since using one affine conversion cannot satisfy making algebraically the content of S-box and corresponding reverse S-box include extra terms as possible as it could be to provide the best resistance against algebraic cryptanalysis[8].

B. The Improved S-box

The enhanced version of AES S-box can be constituted in the sequential three steps.

Step 1. We apply the affine conversion with (5B), (5D) as in equation (4).

$$X = (5B) \times (I) + (5D) \quad (4)$$

Where

(I) ⟶ represents the input byte.

Step 2. We obtain the multiplicative inverse of the output from Step 1 (X) from equation (5).

$$Y = (X)^{-1} \quad (5)$$

Where:

$(X)^{-1}$ ⟶ represents the multiplicative inverse of X over the finite field (28)[14].

Step 3. We apply the same affine transformation, of $\mathcal{L}$ (5B, 5D) to the output from Step 2 (Y) in equation (6).

$$S(I) = (5B) \times (Y) + (5D) \quad (6)$$

Where:

$S(I)$ ⟶ represents the output byte result from an improved AES S-box.

The reverse affine conversion with (0E), (25) is utilized to constitute the enhanced version of reverse AES S-box where [(5B), (5D)] and [(0E), (25)] are the reverse to each other such that satisfy equation (7) for all $x \in G\mathbb{F}(2^8)$.

$$\mathcal{L}(0E, 25)\left[\mathcal{L}(5B, 5D)[x]\right] = x \quad (7)$$

The enhanced version of reverse AES S-box is constituted in the inverse manner of the enhanced version of AES S-box by applying the sequential three steps.

Step 1. We apply the inverse affine transformation $\mathcal{L}$(0E, 25) in equation (8).

$$= (0E) \times (I) + (25) \quad (8)$$

Step 2. We obtain the multiplicative inverse from equation (9).

$$X = (Y)^{-1} \quad (9)$$

Step 3. We apply the same affine conversion, $\mathcal{L}$(0E, 25) again, as in equation (10).

$$I = (0E) \times (X) + (25) \quad (10)$$

The result of utilizing the enhanced version of AES s-box, therefore, efficiently strengthens the sequential cryptographic characteristics.

- The affine conversion period is raised to 16, instead of 4 for traditional AES S-box.
- The repetitive period is raised to 256 instead of fewer than 88 for traditional AES S-box.
- The distance to SAC is decreased to 372 from 432 for traditional AES S-box.
- The number of terms in algebraic content is raised to 255 instead of 9 for traditional s-box, and at the same time the number of terms in the enhanced version of reverse AES S-box is decreased to 253, thus, keeping the number of terms in the algebraic content at approximately the similar amount like in the traditional reverse S-box, which is accurately 255 [9].

Accordingly, a comparison is made between modes of operation when utilizing traditional s-box then when utilizing the enhanced one, and the relative results are depicted.

III. MODES OF OPERATION FOR AES ALGORITHM

DES and AES algorithms are two common techniques under the category of symmetric key enciphering which are widely utilized to encipher a single unit of information such as 128 bits in case of AES algorithm and 64 bits in case of DES algorithms however, practically it is required to encipher message containing multiple units of plaintext. Therefore, the different techniques or methods of encrypting using a block cipher have emerged to encrypt such files consisting of long plaintexts. These different techniques or methods are called modes. Thus, the five modes are briefly illustrated in the following subsequent sections.

A. Electronic Codebook Mode (ECB):

It is the easiest method or way of encrypting any arbitrary length of file or message among all modes hence it is considered the extremely explicit mode of encrypting a file or message among all modes. Each unit is encrypted individually to produce its own ciphertext without intervention or feedback from other units. Equations (11) and (12) illustrate the encryption and the decryption processes, respectively. The encryption and decryption processes are depicted in Fig. 1 and Fig. 2, respectively.

$$C_i = \varepsilon(K, P_i) \quad \text{for } j = 1, \ldots, N \quad (11)$$

$$P_i = D(K, C_i) \quad \text{for } j = 1,...,N \tag{12}$$

The main problem of this method of encrypting messages is that being considered as deterministic process which means that encrypting the identical plaintext units produces the identical ciphertext units in case of using the identical key and that is considered as a drawback that would help a cryptanalyst to disclose the ciphertext by substituting or reordering the units. Therefore, this method is not convenient for supplying the required security for encrypting, for instance, long messages.

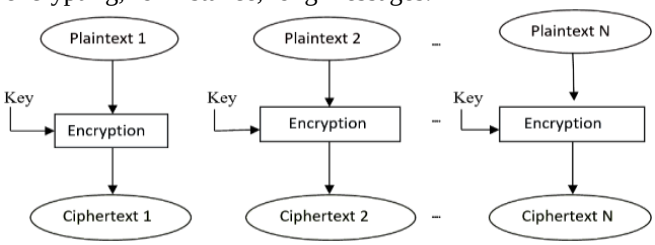


Fig. 1. Encryption Process in ECB Mode

Another disadvantage of this method of encrypting messages is its urgent need to pad the last unit of the message to be the same size as the preceding units in case that the message cannot be divided into an integer number of units with the same size.

Accordingly, the most famous application for which this method can be used is to encrypt messages containing small number of bits, to ensure secure encryption, like, for example, transmitting of key after encryption between the sender and the receiver.

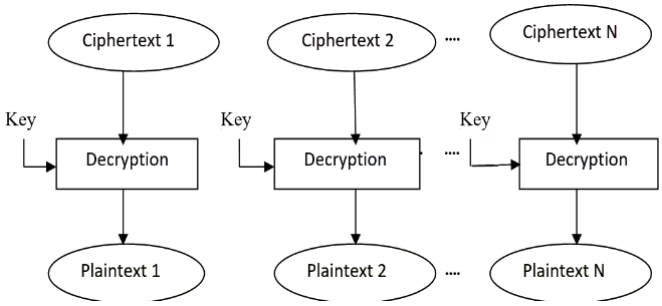


Fig. 2. Decryption Process in ECB Mode

B. Cipher Block Chaining Mode (CBC):

It is considered as an easiest solution to solve the essential problem of ECB mode where the previous unit of outcome is fed back to be XORed with the next unit of income then the output of XOR operation is encrypted using the key which is fixed for all encryption stages to produce the next unit of outcome hence, the stages of encrypting multiple units of plaintext are chained to each other as the name of this technique of encryption implies instead of encrypting each unit individually as ECB mode. Except for the first unit where there is no previous outcome so an initialization vector (IV) is utilized rather than the previous unit of outcome.

This technique provides randomization and make the encryption of multiple units is probabilistic rather than deterministic as the case in ECB mode. Since the output unit of outcome is always fed back as input to produce the next output unit of outcome so the final output unit of outcome is a function of all preceding output units of outcome which means it depends on all preceding output units of outcome thus it is impossible to do the encryption of all units of income at once to increase the speed of the total encryption process which is considered as a deficiency. Another deficiency of this technique of encryption is the accumulation of error in all successive units of outcome in case an error has emerged in one unit of outcome due to using the corrupted unit of outcome as a feedback to produce the next unit of outcome and so on.

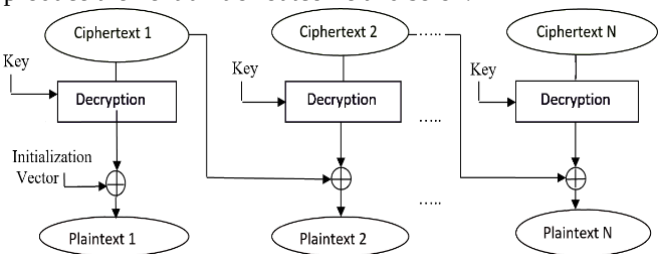


Fig. 4. Decryption Process in CBC Mode

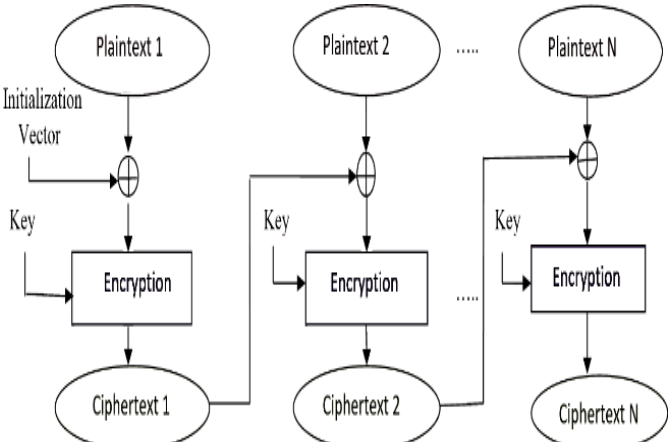


Fig. 3. Encryption Process in CBC Mode

In addition to guarantee that encryption of units of income in this technique of encryption is probabilistic.

IV must be used and must be unique which means to be changed when it is used again for another encryption. However, this technique of encryption suffers from a problem that it requires to pad the last unit of the message to be the same size as the preceding units in case that the message cannot be divided into an integer number of units with the same size as the case in ECB mode. Equations (13), (14), (15) and (16) describe the initial encryption, the successive encryption, the initial decryption, and the successive decryption processes, respectively. The encryption and decryption processes are figured in Fig. 3 and Fig. 4, respectively.

$$C_1 = \varepsilon\left(K, [P_1 \oplus IV\ ]\right) \quad \text{for } j = 1 \tag{13}$$

$$C_i = \varepsilon\left(K, [P_i \oplus C_{i-1}]\right) \quad \text{for } j = 2,...,N \tag{14}$$

$$P_1 = D(K, C_1) \oplus IV \quad \text{for } j = 1 \tag{15}$$

$$P_i = D(K, C_i) \oplus C_{i-1} \quad \text{for } j = 2,...,N \tag{16}$$

C. Cipher Feedback Mode (CFB):

It is considered as one of the techniques that uses the building unit of block cipher to construct the stream cipher which means to transform the block cipher to the stream cipher so that it could benefit from the advantages of the stream cipher such as the stream cipher can execute in real time so the bits can be encrypted and transmitted immediately without delay besides the padding is not required to make the message an integer number of units with the same size as the last two techniques of encryption. The same technique used in CBC mode is also used in CFB mode which is usage of (IV) in enciphering the first unit of income but the difference is the enciphering of (IV) using the key then the output is XORed with the first unit of income to form the first unit of outcome. For the successive units of income, the preceding resulting outcome is used rather than the initialization vector to be encrypted using the same key then the output is XORed with the next unit of income to form the next unit of outcome Therefore this method of encryption is also probabilistic not deterministic as CBC mode hence the encryption of the same unit of income twice results in producing two units of outcome which are different from each other The output unit of outcome in this method of encryption is a function of all previous units of outcome which result in multiple encryption operations for successive units of income cannot be executed in parallel due to using the feedback and also the error is propagated through the subsequent units of outcome when it occurs in any unit of outcome due to using the feedback of previous unit of outcome as the case in CBC mode.

The most important characteristic of CFB mode is that it could acts as a stream cipher hence, the enciphering and the deciphering operations are typically have similar construction thus it does not have to undo the enciphering operation by executing the deciphering operation $E^{(-1)}$ which is in the contrary to ECB and CBC modes where the bits are enciphered and deciphered by executing the enciphering and deciphering operations respectively. That is because the encryption process at the sender is accomplished by employing the XOR operation then the decryption process can just be accomplished by employing again the XOR operation in order to decipher the outcome and to recover the corresponding income at the receiver.

This can be easily proved from equations (17), (18), (19) and (20), which depict the initial encryption, the successive encryption, the initial decryption, and the successive decryption processes in CFB, respectively. The enciphering and deciphering processes are delineated in Fig. 5, Fig. 6, respectively

$$C_1 = P_1 \oplus \left[\varepsilon(K, IV)\right] \quad \text{for } j = 1 \tag{17}$$

$$C_j = P_j \oplus \left[\varepsilon(K, C_{j-1})\right] \quad \text{for } j = 2,...,N \tag{18}$$

$$P_1 = C_1 \oplus \left[\varepsilon(K, IV)\right] \quad \text{for } j = 1 \tag{19}$$

$$P_i = C_j \oplus \left[\varepsilon(K, C_{j-1})\right] \quad \text{for } j = 2,...,N \tag{20}$$

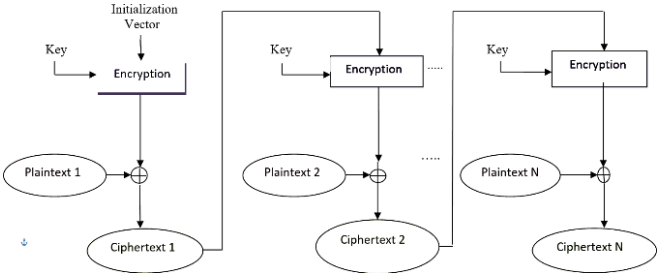


Fig. 5. Encryption Process in CFB Mode

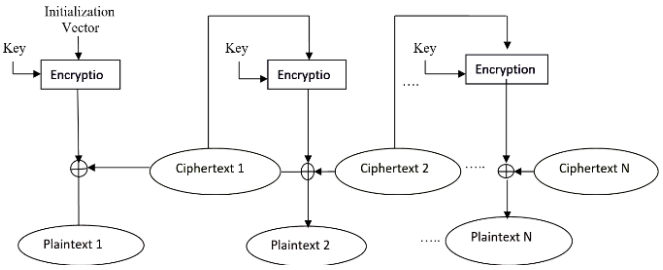


Fig. 6. Decryption Process in CFB Mode

D. Output Feedback Mode (OFB):

It has the same construction of CFB mode except that for OFB mode the encryption function result before XORing with the unit of income to produce the unit of outcome is fed back to be used as an input of the subsequent encryption stage but for CFB mode the unit of outcome itself which results after XORing with the unit of income is fed back to be used as an input in the successive encryption stage. Thus, any output unit of outcome does not depend on any previous units of outcome or income.

Therefore the main advantage of OFB mode is that there is no error accumulation as CFB and CBC modes and if there is an error occurred in encrypting unit of outcome during the transmission, while performing the decryption, it will affect only the corresponding unit of income that will result from decrypting that corrupted unit of outcome individually, which means there is a limited propagation of error. That makes it the most appropriate technique or method for using in communications through channels which has a high probability of noise occurrence like satellite communications. In addition, OFB has a wonderful property that each unit of income can be processed individually without intervention of the previous units of income or outcome thus the output units of outcome can be computed in advance.

Equations (21), (22), (23) and (24) illustrate the initial encryption, the successive encryption, the initial decryption, and the successive decryption processes in OFB mode, respectively. The encryption and decryption processes are depicted in Fig. 7 and Fig. 8, respectively.

$$C_j = P_j \oplus \left[E(K, I_j\right] \quad \text{for } I_j = IV, J = 1 \tag{21}$$

$$C_j = P_j \oplus \left[E(K, I_j\right] \tag{22}$$

for $I_j = E(K, I_{j-1}), J = 2,...,N$

$$P_j = C_j \oplus \left[E(K, I_j \right] \quad (23)$$

for $I_j = IV, J = 1$

$$P_j = C_j \oplus \left[E(K, I_j) \right] \quad (24)$$

for $I_j = E(K, I_{j-1}), J = 2,...,N$

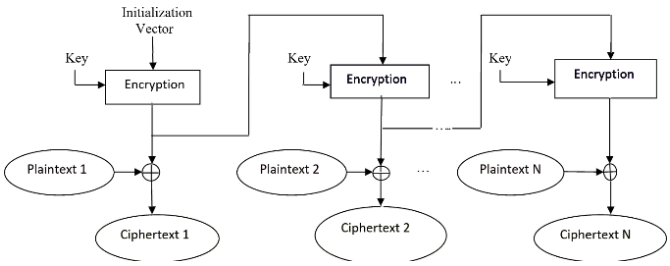


Fig. 7. Encryption Process in OFB Mode

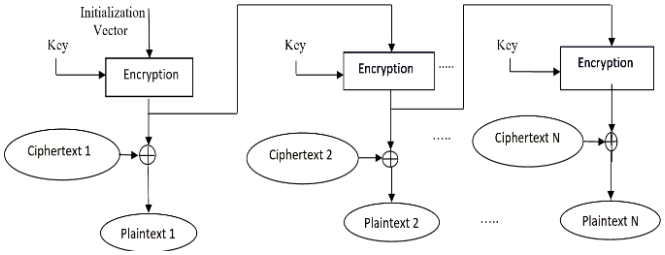


Fig. 8. Decryption Process in OFB Mode

E. Counter mode (CTR):

It is also another technique of encryption which represents originally a block cipher although it can be utilized as a stream cipher as the previous two techniques of encryption. However, the main difference among this technique of encryption from one side and the previous two techniques of encryption from other side that there is no chaining or feedback which subsequently is considered as the major advantage of this technique of encryption over the previous two techniques of encryption. Also, this technique of encryption is better than CBC mode since it has the advantage of being probabilistic as CBC mode and at the same time does not have the disadvantage of feedback as CBC mode.

In fact, this technique of encryption is the only technique which is considered probabilistic and at the same time does not have chaining or feedback. Moreover this technique of encryption is better than ECB mode since it has the advantage of not having feedback as ECB mode and at the same time it does not have the disadvantage of being deterministic as ECB mode but rather it has the advantage of being probabilistic thus the encryption of the same unit of income twice results in producing different units of outcome. As a result, this technique of encryption combines the advantages of ECB mode in addition to advantages of stream ciphers such as CFB and OFB modes as well. The counter is set to specific worth at the first which subsequently will be increased by 1 for each subsequent unit of income such that a different counter is used for each stage of encryption which provides randomization and ensure that encryption is probabilistic not deterministic.

For enciphering, the counter is enciphered after that the XOR operation is performed on the result with the unit of income in order to generate the corresponding unit of outcome. For deciphering, the counter with similar value to the counter of enciphering is enciphered after that the XOR operation is performed again but with the unit of outcome produced in encryption to recover the corresponding unit of income. The most significant advantage of CTR mode is its capability of being executed in parallel due to absence of existing feedback in contrary to OFB and CFB modes. Therefore, all the encrypted units of income in different stages can be executed in parallel at the same time thus increasing the speed of encryption and subsequently the throughput proportionally. Therefore, CTR mode is the most suitable technique among all the preceding techniques of encryption for usage when it is required to fulfill throughput of high degree like for instance high speed networks and is widely used recently in applications such as IP address and ATM which stands for (asynchronous transfer mode) networks.

The mathematical forms of both the encryption and decryption processes in equations (25) and (26). The enciphering and deciphering processes are shown in Fig. 9 and Fig. 10, respectively.

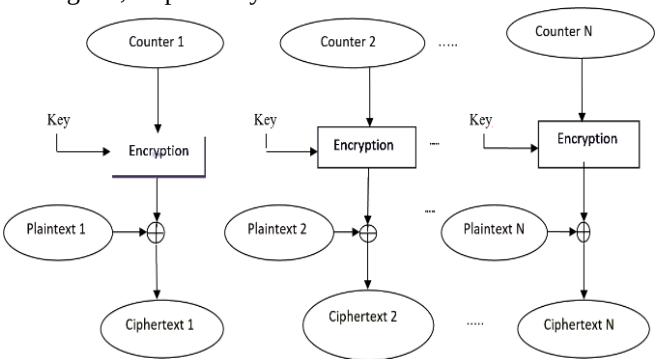


Fig. 9. Encryption Process in CTR Mode

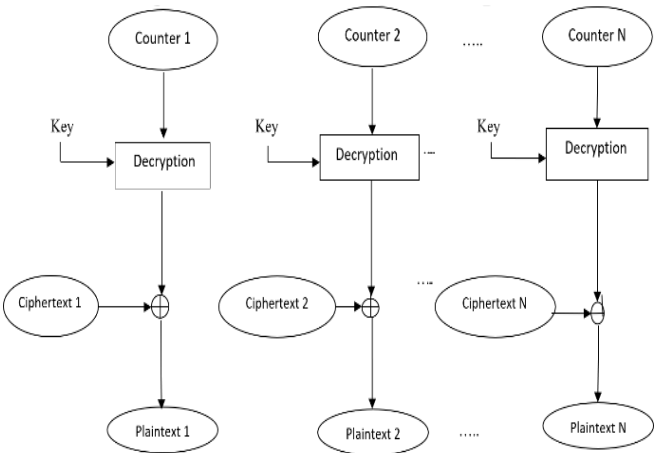


Fig. 10. Decryption Process in CTR Mode

$$C_j = P_j \oplus \left[\varepsilon(K, Co_j) \right] \quad \text{for } j = 1,2,...,N \quad (25)$$

$$P_j = C_j \oplus \left[\varepsilon(K, Co_j) \right] \quad \text{for } j = 1,2,...,N \quad (26)$$

IV. EXPERIMENT ANALYSIS USING MATLAB SOFTWARE

The modes of operation are simulated using MATLAB software to make the performance evaluation based on making a comparison between the modes according to enciphering time and throughput in both traditional S-box for AES and improved AES S-box where encryption time is defined as the time consumed measured in milliseconds between encrypting the first plaintext block (P_1) of the first stage of the mode reaching to produce the final ciphertext block (C_N) of the last stage of the mode, then accordingly find the best mode of operation which requires the minimum time consumption for encrypting and producing the required ciphertext.

Also, throughput is identified as how many bits could be enciphered in one second or in other words it could be called encryption speed measured in Kilobytes per seconds (KB/sec). It is computed as the whole amount of encrypted data divided by the encryption time, and then accordingly finds the best mode of operation which achieves the biggest amount of data encrypted in one second.

The MATLAB software version used in simulation is MATLAB 2014 version and the specifications of laptop used in simulation are as: Core i5, 2.2 GHz processor; 4GB RAM; Windows 10 (64 bit) operating system.

Summary of Experiments

As shown in Table 3, it is concluded that ECB mode takes less time consuming than other modes thus ECB mode is considered the best mode of operation in terms of time consumption in encryption. Then it is noticed that CTR mode consumes the second less time for encryption then CBC mode consumes a third less time for encryption, but the difference between CTR and CBC modes is very small. Finally, it is noticed that OFB then CFB modes are taking the biggest time consumption and therefore are considered the worst modes of operation respectively in terms of time consumption in encryption.

The results of simulation using MATLAB software with respect to time consumption are proposed in Table 3.

Table 3 Time Consumption for Modes of Operation

Mode of Operation	ECB	CBC	OFB	CFB	CTR
Time Consumption (ms)	130	144	149	152	143

Then the throughput of each modes of operation can be calculated where the whole amount of encrypted data is (2KB) and the results are shown in the following Table 4,

Table 4 Throughput for Modes of Operation

Mode of operation	ECB	CBC	OFB	CFB	CTR
Throughput (KB/s)	15.38	13.89	13.42	13.16	13.98

In which it is concluded that ECB achieves the biggest throughput thus ECB is considered the best mode of operation in terms of throughput. Then it is noticed that CTR mode achieves the second-best throughput after ECB mode then CBC mode achieves the third best throughput but the difference between CTR and CBC modes is very small.

Finally, it is noticed that OFB then CFB modes are achieving the smallest throughput and thus are considered the worst modes of operation respectively in terms of throughput. Also, the modes of operation are simulated using MATLAB software to measure the avalanche effect results from changing the plaintext or the key.

For any single input bit of the plaintext or the key, the complement of it should result to change the output ciphertext with probability of one half whenever the position of the single input bit in the plaintext or the key and this condition measures the strength of the enciphering technique. Therefore, in case of changing one bit in the plaintext, each input bit in the plaintext block is complemented from the first position to the last position and the corresponding output cyphertext for each time is compared to the original output ciphertext resulting from the original plaintext before complementing to find the difference which represents the avalanche effect.

Then the same previous scenario has repeated but in case of changing one bit in the key then the average is computed by summation of all changes results from changing the first bit to the last bit in case of the plaintext and in case of the key and divided by the whole size of the plaintext and the key which is 128 bits. The previous simulation is repeated for each mode of the five modes in case of changing one bit in the plaintext and in case of changing one bit in the key by using both the traditional and improved AES S-boxes then the results are taken.

V. EXPERIMENT ANALYSIS USING FPGA

The modes are implemented using FPGA implementation to make performance evaluation and analyze the behavior of each mode according to the enciphering time in both traditional AES s-box and improved AES s- box [15],[16]. The crystal frequency used is 250 MHz with a clock-cycle time of 4 ns.

The ideal average of avalanche effect should be 64 which represents changing 64 bits the half of the output ciphertext (128bit) when complementing one bit whatever its position in the plaintext or the key. Hence, it can be concluded from the results of the average shown in the tables that in case of using the traditional AES S-box CBC is the best mode while ECB and CTR are the worst modes when complementing one bit in the plaintext but when complementing one bit in the key CFB is the best mode while ECB mode is the worst mode. On the other side in case of using the improved AES S-box, CFB is the best mode while OFB is the worst mode when complementing one bit in the plaintext but when complementing one bit in the key CBC and CFB are the best modes while CTR is the worst mode.

VI. CONCLUSION

An analytic study is performed to measure the impact of utilizing five distinctive famous modes on the behavior of "AES" technique with the aid of enciphering time, throughput and strict avalanche criteria (SAC) parameters in the presence of traditional s-box or enhanced S-box formula.

We concluded by the results of our analytic study that SAC parameter is the only criterion by which the impact of utilizing different modes on the behavior of AES technique is apparent however the enciphering time and throughput parameters has no role in exhibiting the influence of utilizing distinctive modes on the behavior of AES technique regardless of formula of the substitution box equation utilized in "AES" technique.10

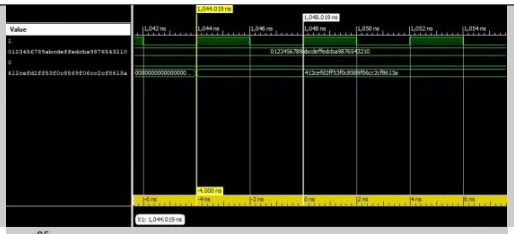
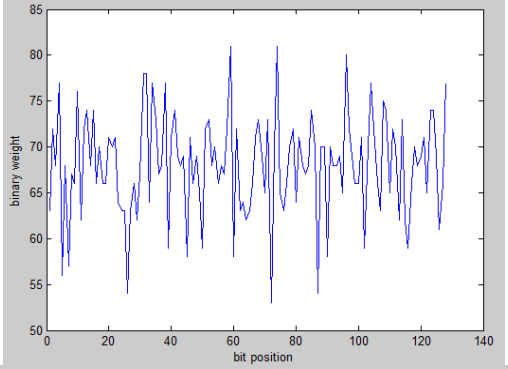
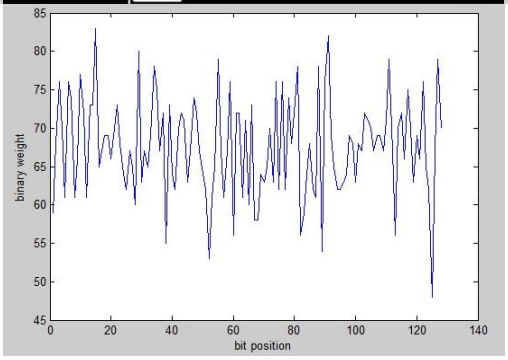
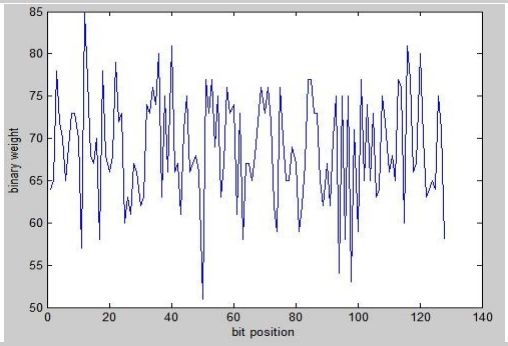
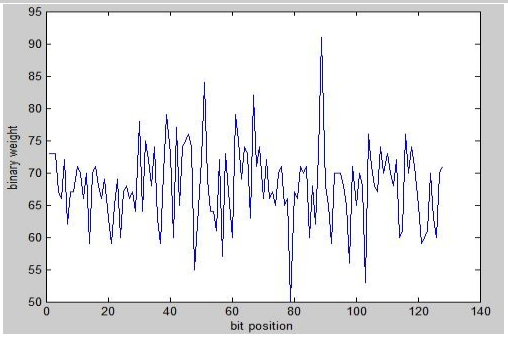
The snapshots of the results for each mode in case of using the traditional s-box and in case of using the improved s-box by applying MATLAB Software and FPGA hardware are represented in the appendices section.

REFERENCES

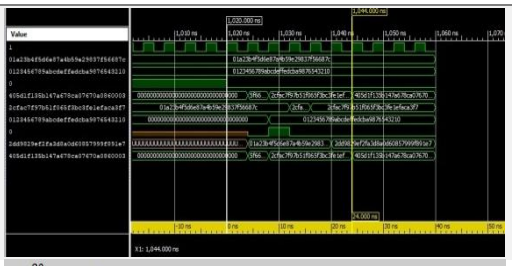
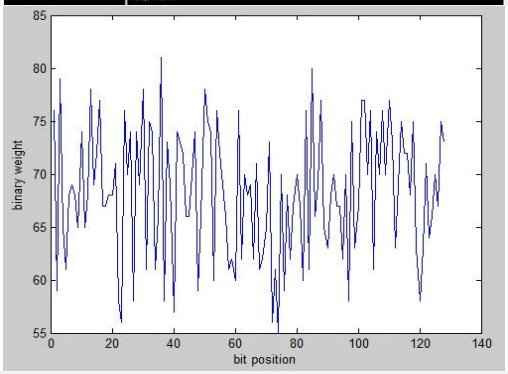
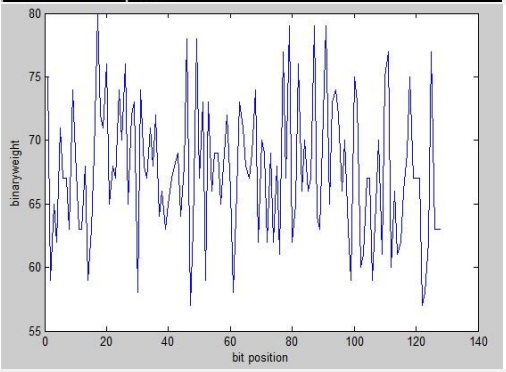
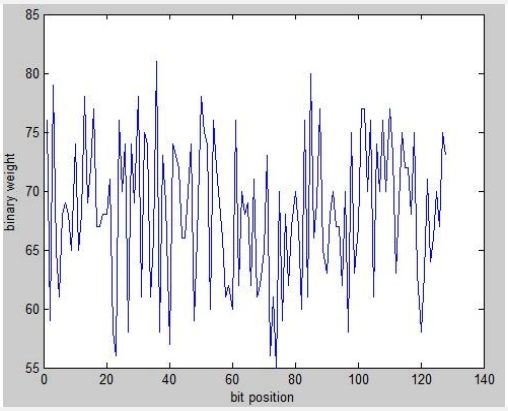
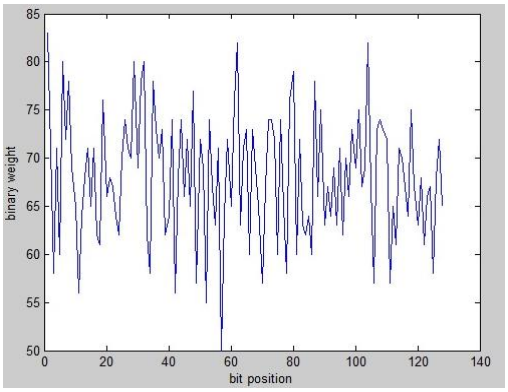
1- S. Ramakrishnan, Cryptographic and Information Security. CRC Press, 2018.
2- J. Daemen and V. Rijmen, "A Specification for Rijndael, the AES Algorithm," 2003.
3- D. Selent, "ADVANCED ENCRYPTION STANDARD," M.S. Progr. Comput. Sci. Rivier Coll., 2010.
4- M. I. Aziz and S. Akbar, "Introduction to cryptography," in Proceedings of the International Conference on Microelectronics, ICM, 2005.
5- D. R. Stinson and S. Tavares, Selected Areas in Cryptography. Springer Verlag, 2012.
6- Christof Paar, Jan Pelzl, Understanding Cryptography, A Textbook for Students and Practitioners, Springer- Verlag, Berlin Heidelberg, 2010.
7- William Stalling, Cryptography and Network Security Principles and Practice Sixth Edition, Pearson Education, Inc, 2014.
8- Lingguo Cui, Yuanda Cao, A New S-Box Structure Named Affine-Power-Affine, International Journal of Innovative Computing, Information and Control (ICIC), June 2007.
9- Jie Cui, Liusheng Haung, Hong Zhong, Chinchen Chang And Wei Yang, An Improved AES S-Box and Its Performance Analysis, International Journal Of (ICIC), May 2011.
10- Mahmoud Al-Fadel, El-Sayed M.El-Alfy, Khaleque Md Ashiq Kamal, Evaluating Time and Throughput at Different Modes of Operation in AES Algorithm, 8th International Conference on Information Technology (ICIT), 2017.
11- Sultan Al-Muhammady And Ibraheem Al-Hejri, A Comparative Analysis ofAES Common Modes of Operation, IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), 2017.
12- R. Avanzi, "A Salad of Block Ciphers The State of the Art in Block Ciphers and their Analysis," Attribution-NonCommercial-NoDerivatives 4.0 International, 2017.
13- L. R. Knudsen and M. J. B. Robshaw, The Block Cipher Companion. 2011.
14- A. Menezes, "Cryptography," in Handbook of Finite Fields, 2013.
15- A. M. Deshpande, M. S. Deshpande, and D. N. Kayatanavar, "FPGA implementation of AES encryption and decryption," in 2009 International Conference on Control Automation, Communication and Energy Conservation, INCACEC 2009, 2009.
16- T. Good and M. Benaissa, "AES on FPGA from the fastest to the smallest," in Lecture Notes in Computer Science, 2005.

APPENDICES

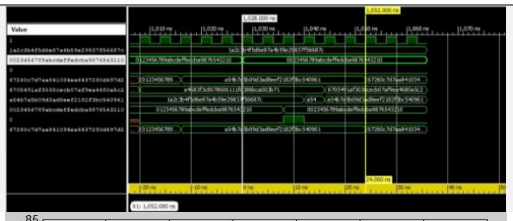
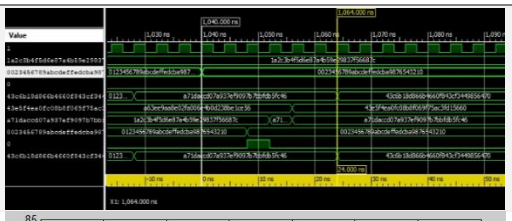
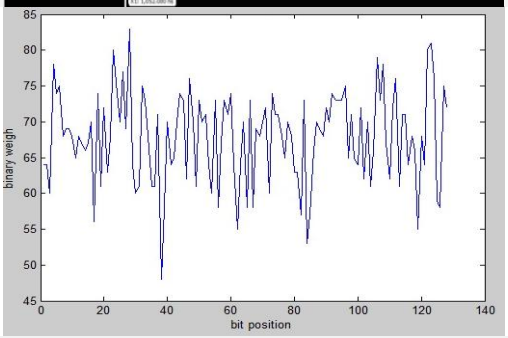
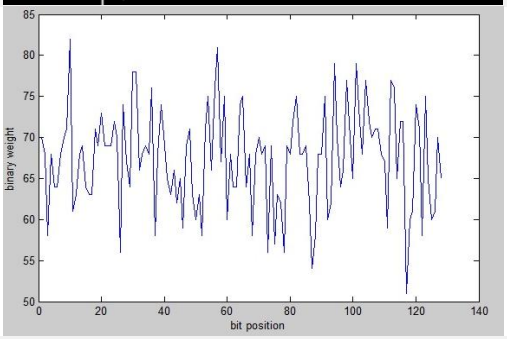
❖ *ECB Mode*

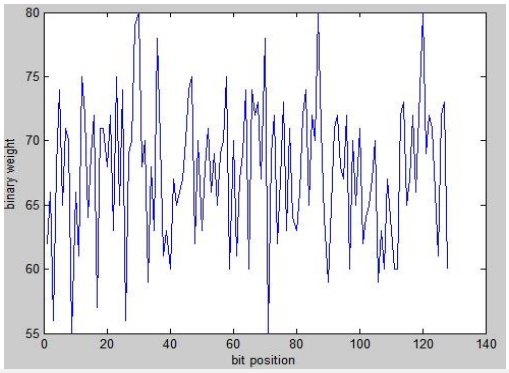
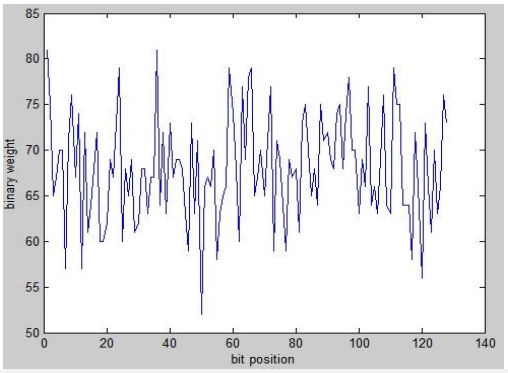
	Old S-Box	*New S-Box*
FPGA implementaton		
Change in Plaintext (Snapshot) MATLAB Implementation		
Average	68	67.5
Change in Key (Snapshot) MATLAB Implementation		
Average	68.8	68.1

❖ *CBC Mode*

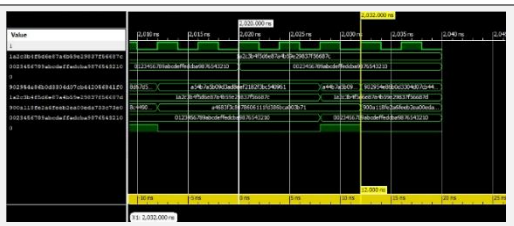
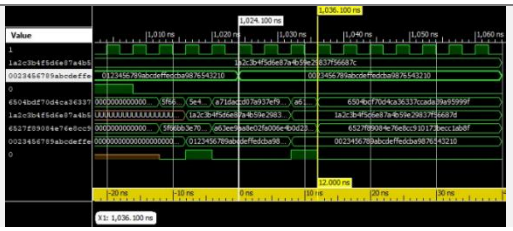
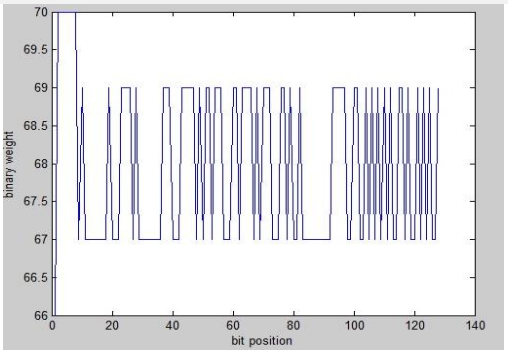
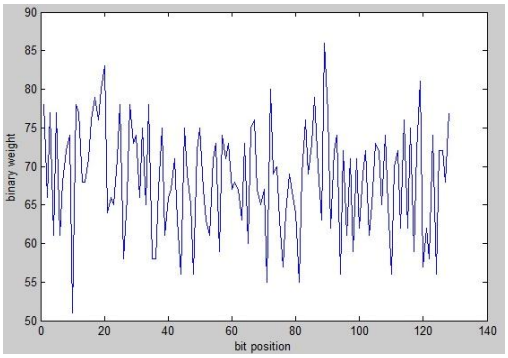
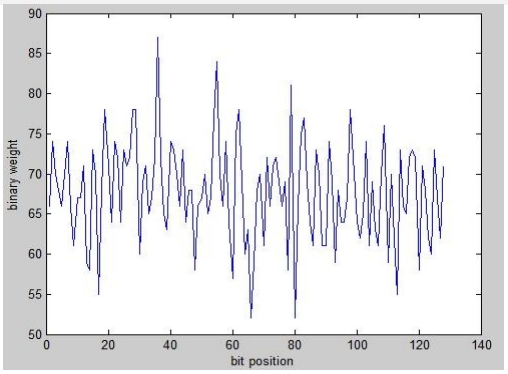
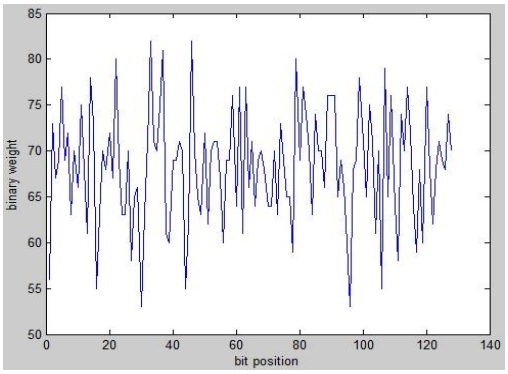
	Old S-Box	*New S-Box*
FPGA implementation		
Change in Plaintext (Snapshot MATLAB Implementation)		
Average	67.4	67.6
Change in Key (Snapshot) MATLAB Implementation		
Average	68.3	68

❖ *CFB Mode*

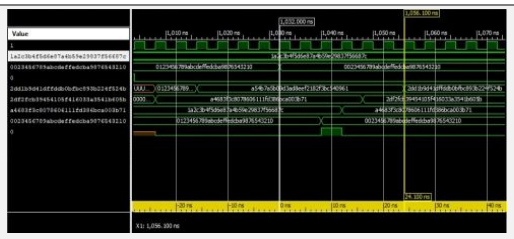
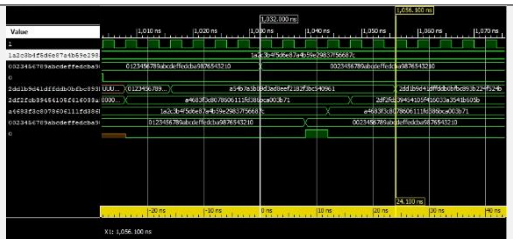
	Old S-Box	*New S-Box*
FPGA implementation		
Change in Plaintext (Snapshot) MATLAB Implementation		
Average	67.9	67.4

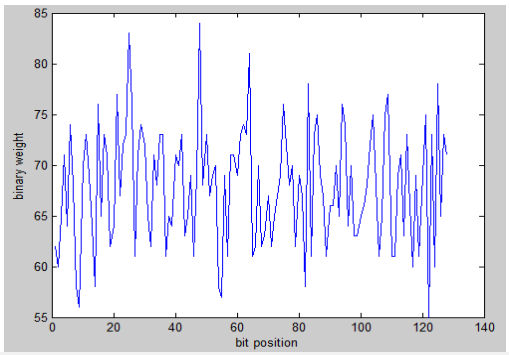
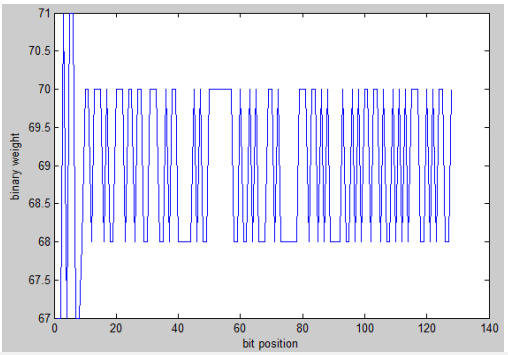
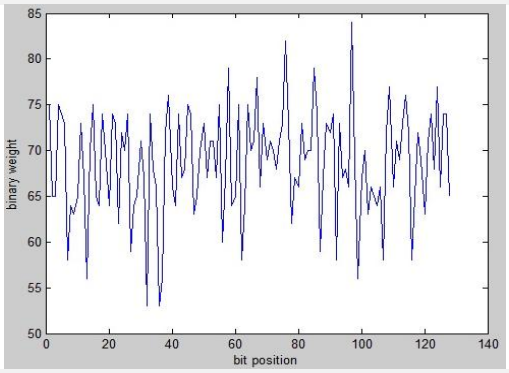
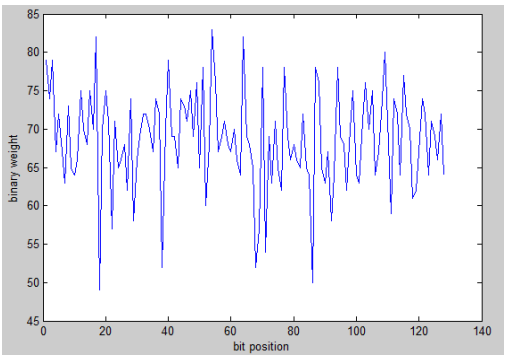
Change in Key (Snapshot) MATLAB Implementation		
Average	67.6	68

❖ *CTR Mode*

	Old S-Box	*New S-Box*
FPGA implementation		
Change in Plaintext (Snapshot) MATLAB Implementation		
Average	68	68.4
Change in Key (Snapshot) MATLAB Implementation		
Average	67.8	68.3

❖ *OFB Mode*

	Old S-Box	*New S-Box*
FPGA implementation		

Change in Plaintext (Snapshot) MATLAB Implementation		
Average	67.9	68.9
Change in Key (Snapshot) MATLAB Implementation		
Average	68.6	68.3