Benha Journal of Engineering Science and Technology
(BJEST)

مجلة العلوم الهندسية والتكنولوجية بكلية الهندسة ببنها

2018; Vol 1-33-45
Journal Homepage:www.bu.edu.eg/bjest

A REVIEW OF ADVANCED ENCRYPTION STANDARD S-BOX PERFORMANCE

Eslam Wahba Afify [1, *], Wageda I. El sobky [2], Abeer Twakol Khalil [3], Mohamed M. EL Faham [4], Reda Abo Alez[5]

[1]Department of Electrical, Faculty of Engineering, Benha University, Egypt,eslam.cv@gmail.com
[2]Department of Mathematics, Faculty of Engineering, Benha University, Egypt, wageda_ibrahim@ bhit.bu.edu.eg
[3] Department of Electrical, Faculty of Engineering, Benha University, Egypt, Abeer.Twakol@bhit.bu.edu.eg
[4]Department of Basic science, Faculty of Engineering, Benha University, Egypt, dr.mmostafa.elfaham@bhit.bu.edu.eg
[5]Department of System and computer Engineering, Faculty of Engineering, Alazhar University, Egypt,Aboalez@gmail.com

Abstract: S-Box plays a major role in the AES algorithm. The strength of S-Box depends on the design and algebraic constructions. This paper provides an overview about AES S-Box analysis, also give idea about different previous research to improve the static S-boxes that has been used in AES, in order to enhance the strength of AES.

Keywords: S-Box, AES, Cryptography, Cryptanalysis, Algebraic Attacks.

الملخص العربى:

الهدف من هذا البحث هو إجراء دراسة استقصائية عن استخدام وتطوير جداول الاستبدال**(S-Box)** فى تحسين قدرة معيار التشفير المتقدم (AES) لمواجهة تحديات الاختراق. وتسليط الضوء على اسلوب التصميم والبناء الجبرى لجداول الاستبدال **(S-Box)** وطريقة الاختراق الجبرى وطرق معالجتة. ويتعرض البحث بالشرح والتوضيح لاهم الابحاث التى تعرض تطوير جداول الاستبدال **(S-Box)** وتحديد افضل الطرق لتحسين تصميم جدول الاستبدال **(S-Box)** وعرض الافكار المستقبليه لتحسين التصميم خاصة ضد الاختراق الجبرى للمعيار التشفير المتقدم (AES).

1. Introduction

All encryption algorithms approved by the National Security Agency (NSA) for ordered handling were, characterized. The quality of any great encryption algorithm is not improved by holding the plan as mystery. In fact, a public domain encryption standard is subject to continuous, expert cryptanalysis. Any leaps forward will probably be accessible to clients and their foes in the mean-time [1]. Block ciphers are a critical and ubiquitous building block of modern cryptography.

DES (Data Encryption Standard) and AES (Advanced Encryption Standard) both are the symmetric block cipher. AES was introduced to overcome the drawback of DES. As DES has a smaller key size which makes it less secure to overcome this triple DES was introduced but it turns out to be slower. Hence, later AES was introduced by the National Institute of Standard and Technology. The basic difference between DES and AES is that in DES plaintext block is divided into two halves before the main algorithm starts whereas, in AES the entire block is processed to obtain the cipher-text. Table (1) discusses some more differences between DES and AES.

Table1. Differences between DES and AES

BASIS FOR COMPARISON	DES (DATA ENCRYPTION STANDARD)	AES(ADVANCED ENCRYPTIO STANDARD)
Basic	In DES the data block is divided into two halves.	In AES the entire data block is processed as a single matrix.
Principle	DES work on Feistel Cipher structure.	AES works on Substitution and Permutation Principle.
Plaintext	Plaintext is of 64 bits	Plaintext can be of 128,192, or 256 bits
Key size	DES in comparison to AES has smaller key size.	AES has larger key size as compared to DES.
Rounds	16 rounds	10 rounds for 128-bit 12 rounds for 192-bit 14 rounds for 256-bit
Rounds Names	Expansion Permutation, Xor, S-box, P-box, Xor and Swap.	Subbytes, Shiftrows, Mix columns, Addround keys.
Security	DES has a smaller key which is less secure.	AES has large secret key comparatively hence, more secure.
Speed	DES is comparatively slower.	AES is faster.

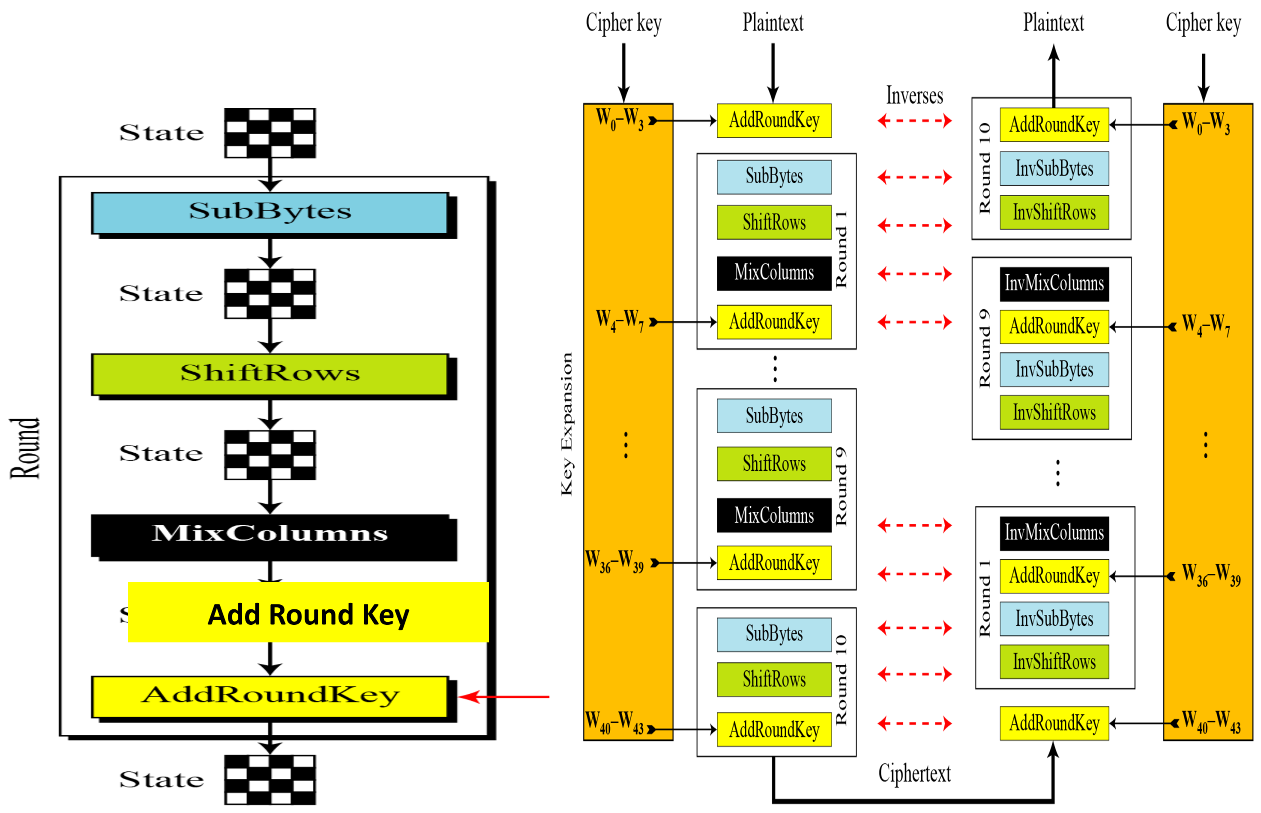
As can be seen from table (1) DES is the older algorithm and AES is the advanced algorithm which is faster and more secure than DES so what is AES?

In August 2000, the Belgian block cipher “Rijndael” was chosen as a champ to be the Advanced Encryption Standard (AES) [2] This occurred in an extraordinary way an open challenge with global cooperation was held by the National Institute of Standards and Technology (NIST) of the United States to discover a successor for the 24-year old Data Encryption Standard (DES). Rijndael is a key-iterated block cipher with an exceptionally rich and solid arithmetical structure. The block and key length are variable in ventures of 32 bits in the vicinity of 128 and 256 bits. The main legitimate information block length for AES is 128 bits that as it may; the key length for AES may be 128, 192 or 256 bits [2,3]. The discussion is primarily centered on Rijndael S-Box although lot of the exchange can likewise be connected to the perfect security of block ciphers and the goal of the crypt-analysis.

The paper is organized as follow: Section (2) gives a detailed analysis of the structure of Advanced Encryption Standard (AES).Section (3) scope in the study of algebraic techniques against block ciphers, gives a detailed analysis of S-Box algebraic structure and characteristics of algebraic resisting attack. Section (4) present the previous researchers developed on S-Box constructions. Conclusion remarks can be found in Section (5).

2. THE STRUCTURE OF AES

The AES is an iterative rather than Feistel cipher [4]. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix Unlike DES, [5] the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. The schematic of AES structure is given in the following illustration plaintext that treated as a byte matrix of size 4x4, where each byte represents a value in GF (2^8). An AES round applies four operations to the state matrix [2]:



(A) (B)

Figure 1: (A) AES one round structure. (B) AES structure.

Sub Bytes: The 16 input bytes are substituted by looking up a fixed table S - box given in design. The result is a matrix of four rows and four columns.

Shift Rows: Each of the four rows of matrix are shifted to the left. Any entries that ‘fall off’ are re-inserted on the right side of row [3].

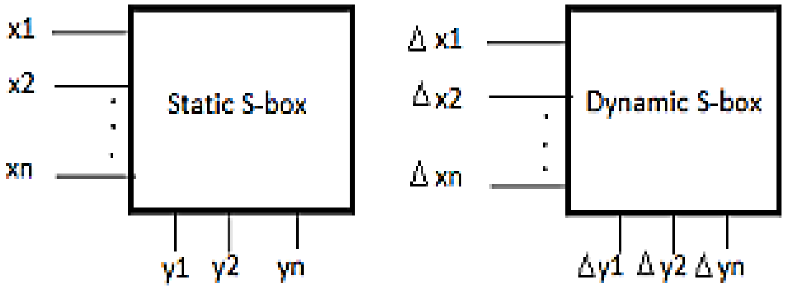
Mix Columns: Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round [4]**.**

Add Round Key: The 16 bytes of the matrix are now considered as 128 bits and are XOR to the 128 bits of the round key. If this is the last round then the output is the cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round [5].

3. The Background of S-Box Generation Algorithms.

The S-Box (substitution Box) is a basic component of asymmetric key algorithms which preform substitution. In block cipher; they are typically used to obscure the relationship between the key and the ciphertext-Shannon’s property of confusion. In general any s-box takes some number of input bits (m), and transforms them into some number of output bits (n), where (n) is not necessary equal to (m). S-boxes can be constructed in two distinct ways: Static and Dynamic. In Static S-box, input vector values are not changed while in Dynamic S-box input vector value changes. Following Static and Dynamic view:

Figure 2: Static and Dynamic S-Box



Properties of Static and dynamic S-box were defined using fig 2. A metric to measure the randomness of data is entropy defined by H (Z) for random variable “z” as follows:
$\mathrm{H(z)} = \sum_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{p(z_i)} \log_2 (\mathrm{z_i^{-1}})$ High entropy means difficult to guess the values. S-box should satisfy better entropy values.

The Rijndael S-Box (substitution box) [6] is a matrix (square array of numbers) used in the Advanced Encryption Standard (AES) cryptographic algorithm. Is serves as a lookup table. Substitution is a nonlinear transformation which performs confusion of bits. S-Box is represented as a 16x16 array, rows and columns indexed by hexadecimal bits [7].

A structure of AES S-Box regarding 8 bit bytes as elements in GF (2^8), AES S-Box is a combination of a power function *f*(*x*) (the multiplicative inverse modulo the irreducible polynomial
$x^8 + x^4 + x^3 + x + 1$, which is denoted in binary by 0x11b) and an affine transformation *l*(*x*) [8],

where.

$$f(x) = \begin{cases} (x^{-1}), & x \neq 0 \\ 0, & x = 0 \end{cases} \qquad (1)$$

$$I(x) = \begin{bmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{bmatrix} \times \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \qquad (2)$$

WhereX_i's are the coefficients of x (i.e., the bits of the bytes), and x_0 is the least significant bit.

From the above description, we can derive the AES S-Box algebraic expression [7]:

$$(x) = 05x^{FE} + 09x^{FD} + F9x^{FB} + 25x^{F7} + F4x^{EF} + 01x^{DF} + B5x^{BF} + 8Fx^{7F} + 63 \qquad (3)$$

The coefficients and exponents of algebraic expression are all in hexadecimal. The coefficients of algebraic expression of the AES inverse S box are shown in Table (1).

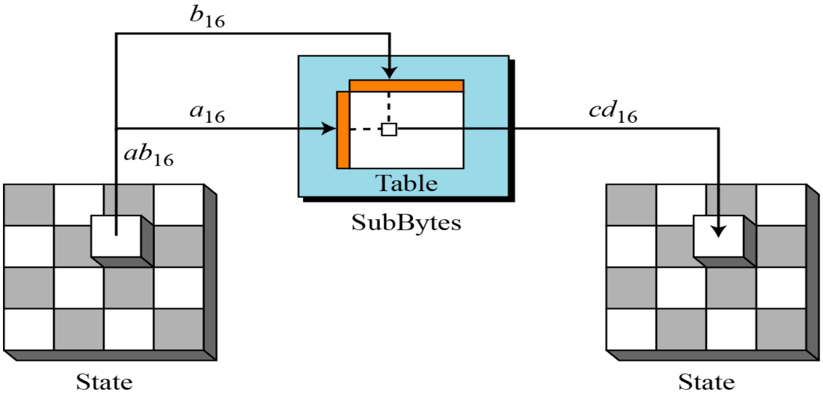


Figure 3: SubBytes and InvSubBytes processes

The exponents of algebraic expression are all divided into two parts in hexadecimal that are listed in column 1 (m denotes the higher bits) and row 1 (n denotes the lower bits), respectively [9, 10]. The rest of the elements in Table 2 are coefficients corresponding with the exponents of algebraic expression in hexadecimal. So, the algebraic expression of AES inverse S-Box is similar to:

$$y = 05x^{fe} + cfx^{fd} + \ldots + f3x + 52 \qquad (4)$$

From Equation (3) and Table (2), it is easy to see that the algebraic expression of AES S-Box is so simple that only 9 terms are involved, while the AES inverse S-Box reaches 255. The simple algebraic expression of AES S-Box is the most interesting and disadvantageous properties. Although no efficient attack has been found about it up to now, the simple algebraic expression is always regarded as the foundation for cryptanalyzing AES. The principles and modules are adopted by many block ciphers since Rijndael was selected as AES. We call this kind of S boxes AES-like [8].

Table2. Coefficients of algebraic expression of the AES S-Box (Hex)

m,n	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

3.1 Algebraic property of s-box.

One S-Box with good cryptographic properties can ensure the cipher to resist against a variety of cryptanalysis methods, so any shortcomings of S-Box will weaken the security of the cipher [10]. AES S-Box is a $\mathbf{8}\times\mathbf{8}$ Boolean function, and these 8 Boolean functions condition and affect each other. Even if these 8 functions have some properties simultaneously, the S-Box Boolean function may have not the similar properties [9]. Therefore, it is necessary to analyze the algebraic properties of S-Box function.

3.2 Algebraic cryptanalysis of S-box

The goal of algebraic cryptanalysis is to break cryptosystems by using mathematical tools coming from symbolic computation and modern algebra [11]. More precisely, an algebraic attack can be decomposed in two steps: ***first*** the cryptosystem and its specifics have to be converted into a set of multivariate polynomial equations, ***second*** the solutions of the obtained polynomial system have to be computed. The security of a cryptographic primitive thus strongly relies on the difficulty of solving the associated polynomial system.

These attacks have been turned out to be extremely productive for both public key or symmetric cryptosystems; block and stream ciphers. Since successful Gröbner basis attacks on block ciphers are conceivable, it must be contemplated precisely how Gröbner basis algorithms depend on the structure of polynomial systems corresponding to block ciphers. One of the possible approaches is based on the notation of semi-regular sequences of polynomials one of the conceivable methodologies depends on the documentation of semi-normal groupings of polynomials [7, 8]. Using the AES as an example, we have considered three algebraic representations for block ciphers. It was proved that the AES polynomial equations over GF (2^8) are not semi-regular, and that the AES systems of quadratic equations (QM) over GF (2) are not semi-regular over GF (2).

Definition3. [10] Given r equations of t terms in GF (2^8), the resistance of algebraic attacks (RAA) s denoted by r and is defined to

$$\mathrm{r} = \left({(t-r)} \;/\; {n} \right)^{\left({(t-r)}/{n} \right)} \qquad (5)$$

Be For AES S-box,$t = 81, r = 23, n = 8$, we can obtain $\mathrm{r} \approx 2^{22.9}$. Jung [11] claimed (Γ) should be greater than 2^{32} for secure ciphers. While AES S-Box has $\mathrm{r} = 2^{22.9}$, it can be a weakness of AES.

Note this measure depend mainly on taking multiplicative inverse. For the improved AES S-box, we can obtainr $\approx 2^{22.9}$.

Note Any S-Box where each output is produced by a bent function of input bits, and where any liner combination of the output bits is also a bent function of the input bits, is a perfect S-Box.

4. Previous Research

Previous researchers developed several S-Box constructions which will be discussed in the following lines by considering the scope of algebraic attacks.

Kazlauskas [5] proposed a new algorithm which is capable of generating a key dependent S-Box to avoid linear and differential cryptanalysis due to static S-box. They have also introduced a modification in Key Scheduling algorithm, where substitution of bytes is omitted from the round keys generation. In addition, they have shown that independency measure ratio of S-Box generated by their algorithm is roughly identical to model ratio for independent and individual numbers. Moreover, main advantage of their approach is to be able to generate numerous S-boxes by changing the secret key. However, the proposed algorithm consumes significant amount of time to generate dynamic S-boxes.

Alamsyah et al. [10] presented a novel S-Box that uses irreducible polynomial $m(x) = x^8 + x^6 + x^5 + x + 1$ with an additional constant 8-bit vector (00000001). The strength of their S-Box was tested using balance, bijective, nonlinearity, SAC, and BIC (BIC-nonlinearity). The results of the testing show that the proposed S-Box was a balanced and was bijective. The testing also gave the average nonlinearity of 112, the average SAC of 0.4995, and the average BIC-nonlinearity of 112. These results indicate that the proposed S-Box had better security level compared to other existing S-boxes.

Wei Yang et al [11] shown that by adding an affine transformation before taking multiplicative inverse, the complexity of both AES S-Box algebraic expression and the inverse S-Box algebraic expression can be further improved. The number of terms in AES S-Box algebraic expression is increased from 9 to 255, and the number of terms in inverse S-Box algebraic expression is increased from 9 to 253. So the vulnerability of only 9 terms in AES S-Box algebraic expression and the inverse S-Box algebraic expression can be avoided.

Wang and liu [12] proposed an improved S-Box by exchanging order of taking multiplicative inverse and applying affine transformation. The algebraic expression of the S-Box involves 255 terms, and its distance to SAC is 408. However, this method has some drawback such as the algebraic expression of the inverse S-Box involves only 9 terms. The algebraic expression of the inverse S-Box is too simple. Moreover, its affine transformation period is still 4, and its iterative period is still less than 88. So the S-Box has almost the same cryptographic properties with AES S-box.

Gupta and Sarkar [13] presented two new techniques to generate non-linear resilient S-boxes and proved that the correlation immunity of the resilient S-boxes is preserved under composition with an arbitrary Boolean function. However, their techniques were not resistant to the algebraic attacks.

Fahmy et al. [14] introduced a technique to generate key dependent S-Box especially for AES, which can be generated from the secret key with the help of two linear congruence parameters of ISO-C Standard and GNU-C respectively. They further tested their algorithm for measuring randomness and found satisfactory results. But, their technique has completely replaced original S-Box with new dynamic S-Box and eliminated the Inverse S-box, which was the complete violation of AES design.

Lingguo and Yuanda [15] discussed the problem of the simple algebraic structure of AES S-Box. By resolving the reason why the algebraic expressions of AES-like S-boxes are so simple, they draw a conclusion that (n + 1) items can be involved in the algebraic expression of AES-like S-Box in GF (2^n) at most. Then, a new S-Box structure named APA is designed such that the algebraic complexity is increased. As an application, they improve AES S-Box with the APA structure. It has been demonstrated that not only the algebraic complexity of AES S-Box is increased from 9 to 253 and its inverse S-Box keeps 255, but other good cryptographic characteristics of AES S-Box are inherited.

Krishnamurthy and Ramaswami [16] presented an idea to modify the original structure of AES with an inclusion of one additional state named as Rotate S-Box at the beginning of each round, while decryption had only four states where Inverse Substitute Bytes were tweaked to nullify the effect of Rotate S-Box state used in encryption. They successfully depicted that the extra time required for an extra state and tweaked Inverse Substitute Bytes is negligible and their algorithm was immune to cryptanalysis.

Janadi and Tarah [17] stated that AES was designed to resist probabilistic attacks but is more suitable to algebraic attacks after the disclosure of XSL (extend end Sparse Linearization) attack. So, they proposed a modification in the generation of S-boxes by mixing each value of the static S-Box with a value generated by MD5 (Message Digest) hash function. They have also tested their proposal using statistical tests and concluded that their algorithm do not violate any security credentials.

Stoinov [18] proposed another design where four different S-boxes could be used in the encryption process. He used both original S-box, and original Inverse S-Box to generate two additional S-boxes on the basis of taking left and right diagonals as axis of symmetry followed by changing the location of corresponding bytes. Moreover, he had successfully tested newly generated S-boxes for balancing, non-linearity, strict avalanche criterion, low XOR table, diffusion order, invariability, and concluded that all four S-boxes could be used for encryption and their Inverse S-boxes could be used for decryption without compromising the security. The actual downside of this design was to use pre calculated S-boxes, which do not depend directly upon the secret key or round keys.

Gong at el. [19] proposed an AES implementation on the basis of five lookup tables generated from original S-box. The advantages include reduction in the code-size in comparison to original AES and improvement in efficiency of implementation. Although, this design was significantly proficient on FPGA devices, yet it contradicts primitive structure of AES and was not tested against any of the statistical tests.

Juremi et al. [20] designed an AES like design for key dependent S-boxes using rotation. They carefully manifested how the property of S-Box rotation can be used to create key dependent S-boxes from round keys. The cipher structure of proposed algorithm resembles original AES and with an addition of key dependent S-Box without changing its values. Further, modified AES algorithm does not contradict the security and design parameters of original AES, as all of the mathematical criteria were kept unchanged.

Hosseinkhani and Javadi [21] introduced a key dependent S-Box generation algorithm which was resilient to linear and differential cryptanalysis. They had further performed some experiments on their algorithm to deduce that it improves the security of original AES without modifying any on the original design criteria and is capable of generating numerous S-boxes.

Sahoo et al. [22] proposed to utilize a different affine transformation in the creation of static S-boxes to be used in encryption and decryption. Implementation time had been calculated experimentally for S-Box generation using standard and newly proposed affine transformation. It had been deduced that time taken to generate the S-Box is slight improved. But, no attention had been paid to test the proposal against any of the security metrics. Consequently, minute advantage in execution time cannot neutralize lack in cryptographic strength.

Nadaf and Desai [23] proposed an algorithm which was able to generate key dependent S-boxes and were optimized to run on FPGA devices. The proposed algorithm does not contradict any design property and is able to encrypt faster on the hardware with resilience to linear and differential cryptanalysis.

Hussain et al. [24] presented a new technique based on affine-power-affine transformation, which can generate S-boxes with the property of additional complexity in nonlinear mappings. In addition, authors have tested their technique using nonlinearity analysis, linear approximation analysis, and differential approximation analysis, bit independent criterion and strict avalanche criterion and conclude that modified technique was capable to resist cryptanalysis.

Das at el. [25] successfully shown that different irreducible polynomial and different additive constants in GF (2^8) can also be employed to generate S-boxes. After conducting some experiments and NIST statistical tests they have concluded that most of the irreducible polynomials and additive constants were even generating better S-boxes than the original S-Box. Further, the usage of different polynomials and additive constants could be made key dependent in order to neutralize the threat of internal trap door or cryptanalysis.

Waqas at el. [26] tried to alter the Affine matrix used in the primitive AES with numerous other alternative affine matrices and found out that there are some good matrices that have no repeated entries and even no fixed points. They had further tested the S-Boxes generated by good matrices by employing strict avalanche criterion, avalanche effect, bit independence criteria and nonlinearity measurements. Further, they had proved that there are some matrices which were capable of generating even more complex S-boxes in comparison to the S-Box used in AES.

Azzawi [27] proposed the generation of dynamic S-Box by fusing the output of three keys using an exclusive OR operation. Two out of those three keys have been generated using a random number generator and again an exclusive OR operation is applied on the output generated by fusion operation and the multiplicative inverse of each byte before performing affine operation. In addition to that author has also proved that the proposed algorithm's avalanche effect was marginally on the higher side in comparison to original AES and is capable of preventing cryptanalysis and brute force attacks.

Wenceslao [28] completely revamped AES with the use of multiple S-boxes to replace Mix Columns transformation with a novel Substitute Bytes XOR transformation. They had further shown that the efficiency of encryption had been escalated and efficiency of decryption had been proliferated in comparison to basic AES. But, at the same time avalanche effect has been plummeted to below acceptance rates for the samples differ by one bit.

Yurii Gorbenko et al. [29] present the optimization of the known S-Box generation method with high nonlinearity, based on the time minimization of S-Box checking for compliance with the set of criteria. The presented approach allows the order determination of the selection criteria application in which the checking time of S-Box will be minimal. Two variants of the optimal order of the criteria application on the S-boxes generation were proposed. Software implementation on a single PC allows to reach average 30 minutes generation time for a permutation of (2^8) degree with nonlinearity 104.
In fact the utilization of S-Boxes is one of the main strength of any block cipher system, since both linear and differential cryptanalysis require the known S-boxes. So, researchers have mainly focused on the primitive AES in order to enhance the strength of AES.

So our article schedule most research offers that had been done by researcher by years, this article selects three type of S-Box that improved based on algebraic structure [1, 9, 30]. In order to make comparison, the cryptographic properties of AES S-Box and the improved AES S-Box are comparison [1, 9, 30]. Performance comparison results are given in Table (3).

Table3. Comparisons of cryptographic properties of S-boxes [9]

Performance index	**AES S-box[1]**	**Affine-Power-Affine AES S-Box [30]**	**Improved S-box[9]**
Balance criteria	balance	balance	balance
Differential uniformity$\delta(F)$	4	4	4
Non-zero linear structure	none	none	none
Resistance of algebraic attacks г	$2^{22:9}$	$2^{22:9}$	$2^{22:9}$
Distance to SAC	432	804	372
Non linearity N(F)	112	112	112
Number of terms in S-box algebraic expression	9	255	255
Affine transformation period	4	4	16
Iterative period	less than 88	less than 88	256
Number of terms in inverse S-box algebraic expression	255	9	253

As can be seen from Table (3), the Strict Avalanche Effect criterion DSAC of the improved AES S-Box is reduced. That is, the improved AES S-Box has a better performance in Strict Avalanche Effect criterion (SAC) than AES S-Box and the S-Box Affine-Power-Affine (APA) [31]. The number of terms in the improved AES S-Box algebraic expression is increased, and the improved AES inverse S-Box algebraic expression has almost the same number of terms as AES inverse S-box. It can greatly avoid vulnerability of only 9 terms not only in AES S-Box algebraic expression, but also in the inverse S-Box Affine-Power-Affine (APA) algebraic expression. The affine transformation period is increased, so the improved AES S-Box has better performance in affine transformation than AES S-Box and the S-Box (APA). The iterative period of the improved AES S-Box is increased. In short, the improved AES S-Box has better cryptographic properties. By substituting AES S-Box with the improved AES S-box, it can be easily applied to AES.

We suggest that the complexity of construction principle and algebraic expression of design S-Box is helpful to improve the security of AES against algebraic attack.

5. CONCLUSIONS

In this review study, spot on different S-Boxes developments to determining the best S-Box to use in any encryption algorithms (particularly The AES encryption which is widely used and most popular encryption standard). It presents complete study and scope three type of existing S-Box by performance analysis and comparative Performance study as can be seen from table (3). By research and study analysis, paper finds that algebraic attack is most security hole of AES S-Box and suggest that improve S-box by enhancement algebraic properties and Resistance Algebraic Attack (RAA).in future work to generate strong S-Box, S-Box equation system must has strong (RAA).

6. References

[1] Daemen, J. and V. Rijmen, The Design of RIJNDAEL: AES The Advanced Encryption Standard, Springer-Verlag, Berlin, 2002.

[2] Y.-S. Yeh, C.-Y. Lee, T.-Y. Huang and C. H. Lin, A transposition advanced encryption standard (AES) resists 3-round square attack, International Journal of Innovative Computing, Information and Control, vol.5, no.5, pp.1253-1264, 2009.

[3] William Stallings, "Cryptography and Network Security", 6th Edition, Pearson Education, 2013.

[4] https://en.wikipedia.org/wiki/Rijndael_S-box.

[5] Kazys KAZLAUSKAS, Jaunius KAZLAUSKAS, "Key Dependent S-Box Generation in AES Block Cipher System," INFORMATICA, vol. 20, no. 1, pp. 23–34, 2009.

[6] A.M.Leventi-Peetz and J.V.Peetz, "Generating S Box Multivariate quadratic equation Systems and Estimating Algebraic Attack Resistance Aided by Sage Math "Godesberger Allee 185-18, DE53175 Bonn, Germany ,June ,2015

[7] https://www.tutorialspoint.com/cryptography/block_cipher_modes_of_operation.htm

[8] https://www.webopedia.com/TERM/C/cryptanalysis.html

[9] Jie Cui, Liusheng , Hong Zhong , Chang and Wei Yang ,"An Improved AES-S Box And Its Performance Analysis" International Journal of Innovative Computing information and Control, volume 7 ,number 5 A, MAY 2014

[10] Alamsyah; Agus Bejo; Teguh Bharata Adji,"AES S-box construction using different irreducible polynomial and constant 8-bit vector", IEEE Conference on Dependable and Secure Computing,2017.

[11] Liu, J., B. Wei and X. Wang, Affine transformation observation on Rijndael S-box, Journal of Xidian University, vol.32, no.1, pp.94-97, 2005.

[12] Jingmei Liu, Baodian Wei, Xiangguo Cheng and Xinmei Wang, "An AES S-Box to increase complexity and cryptographic analysis", In the proceedings of 19International conference on Advanced Information Networking and Applications, pp.724-728, 2005.

[13] Kishan Chand Gupta and Palash Sarkar, "Improved Construction of Non-linear Resilient S-Boxes", IEEE Transactions on Information Theory, Vol. 51, No.1, pp.341358, 2005.

[14] A. Fahmy, M. Shaarawy, K. El-Hadad, G. Salama and K. Hassanain, "A Proposal for a Key-Dependent AES", In the proceedings of 3rd International Conference on Sciences of Electronic, Technologies of Information and Telecommunications, Tunisia, 2005

[15] Lingguo Cui and Yuanda Cao "A New S-Box Structure Named Affine-Power-Affine" International Journal of Innovative Computing, Information and Control Volume 3, Number3, June2007.

[16] Krishnamurthy G N and V Ramaswami, "Making AES Stronger: AES which Key - Dependent S-Box", International Journal of Computer Science and Network Security, Vol. 8, No. 9, pp. 388-398, 2008.

[17] Aida Janadi and D. Anas Tarah, "AES Immunity Enhancement against algebraic attacks by using dynamic S-Boxes", In the proceedings of 3rd International Conference on Information and Communication Technologies: From Theory to Applications, 2008.

[18] Nikoli Stoinov, "One Approach of using Key-Dependent S-BOX in AES", In the proceedings of 4th International conference, Multimedia communications, Services and Security - Communications in computer and information science, Vol. 149, pp. 317323, 2011.

[19] Jin Gong, Wenyi Liu and Huixin Zhang, "Multiple Lookup Table-Based AES Encryption Algorithm Implementation", In the proceedings of International conference on Solid State Devices and Materials Science, pp. 842-847, 2012.

[20] Julia Juremi, Ramlan Mahmod, Salasia Sulaiman and Jazrin Ramli "Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key" International Journal of Cyber-Security and Digital Forensics, Vol. 1, No. 3, pp. 183188,2012.

[21] Razi Hosseinkhani and Hamid Haj Seyeed Javadi, “Using Cipher Key to Generate Dynamic S-Box in AES Cipher System”, International Journal of Computer Science and Security , Vol. 6, No. 1, pp. 19-28, 2012.

[22] Oyshee Brotee Sahoo, Dipak K Kole and Hafizur Rahman, “An Optimized S-Box for Advanced Encryption Standard (AES) Design”, In the proceedings of International Conference on Advances in Computing and Communications, pp. 154-157, 2012

[23] Reshma Nadaf and Veena Desai, “Hardware Implementation of Modified AES with Key Dependent Dynamic S-Box”, In the proceedings of International Conference on Advanced Research in Engineering and Technology, pp. 576-580, 2012.

[24] qtadar Hussain, Tariq Shah, Muhammad Asif Gondal and Hassan Mahmoud, “S8 affine-power-affine S-boxes and their applications”, Neural Computing and Applications, Vol. 21, No. 1, pp. 377-383, 2012.

[25] S. Das, J.K.M.S. Uz Zaman and R. Ghosh, “Generation of AES S-Boxes with various modulus and additive constant polynomials and testing their randomization”, In the proceedings of International Conference on Computational Intelligence: Modeling Techniques and Applications, pp. 957-962, 2013.

[26] Umer Waqas, Shazia Afzal, Mubeen Akhtar Mir and Muhammad Youssef, “Generation of AES like S-boxes by Replacing Affine Matrix”, In the proceedings of 12International Conference on Frontiers of Information Technology, pp. 159.164, 2014.

[27] Hasan M. Azzawi, “Enhancing The Encryption Process of Advanced Encryption Standard (AES) By Using Proposed Algorithm to Generate S-Box”, Journal of Engineering and Development, Vol. 18, No. 2, 2014.

[28] Felicisimo V. Wenceslao, Jr. “Performance Efficiency of Modified AES Algorithm using Multiple S – Boxes”, In the proceedings of International Journal of New Computer Architectures and their Applications, Vol. 5, No. 1, pp. 1-9, 2015.

[29] R. O. a. Y. G. Mariia Rodinko, "Improvement of the High Nonlinear S-Boxes Generation Method," Third International Scientific-Practical Conference Problems of Info communications. Science and Technology ©2016 IEEE vol. 978, 2016.

[30] J. M. Liu, B. D. Wei and X. M. Wang, One AES S-Box to increase complexity and its cryptanalysis Journal of Systems Engineering and Electronics, vol.18, no.2, pp.427-433, 2007

[31] https://techdifferences.com/difference-between-des-and-aes.html