International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Algebraic Construction of Powerful Substitution Box

Eslam wahba afify, Wageda I. El sobky, Abeer T. Khalil, Reda Abo Alez

Abstract: ***The development of wireless transmission, day by day contacts the new statures of innovation. Cryptography is one of the procedures used to give security to information streaming over the system by encryption and decryption. Substitution box (S-box) is a one of a kind nonlinear activity in Advanced Encryption Standard (AES), this paper proposed a new algebraic approach to build the multifaceted nature of S-box by changing the affine transformation. This builds the affine change period to end up 102 and expands the security of the S-box against algebraic attacks and interpolation attacks. Further examination has uncovered that the Operational multifaceted nature of the power S-box is higher than the essential S-box. the proposed powerful S-box satisfies the ideal property of Avalanche's impact and has more prominent security towards linear and differential cryptanalysis. New S-box acquires all focal points and efficiency of any current advanced usage of AES S-box***

Keywords: Boolean Function, Advanced Encryption Standard (AES), Substitution Box (S-box), Irreducible Polynomial, Nonlinearity, Strict Avalanche Criterion (SAC), Bit Independent Criterion (BIC), an affine period.

I. INTRODUCTION

Advanced Encryption Standard (AES) is a symmetric block cipher that is broadly utilized in encoding information by various associations to make secure their information from being hacked. Various schemes have been created to assault it. Be that as it may, There has been no effective attack on full AES until now. The main non-linear part of the AES is the S-box, which generates confusion in the algorithm and in this way assumes a significant task in their safety. Which the primary core of fascination for the cryptanalysis is to examine the soft spot for specific assaults. Since 2000 onwards a few algebraic assaults on AES have been done, which verified the security of AES. And yet, various investigates have been finished for making AES progressively secure by improving S-boxes to give more confusion to the cryptanalyst.

A superior and systematic technique to produce those entries in the S-boxes is by building a nonlinear Boolean function, mapping (n) input bits to (m) yield bits. There are other criteria that must be met in structuring the S-boxes. By comprehension make cryptographically good S-boxes. Numerous cryptanalysts have studied the essential properties of AES. For example, in [1] introduced a straightforward strategy that serves both ways. This technique is based on the synthesis of symmetrical assembly work on the Galois field and inversion map. The improvement methodology gives an enormous number of non-linear elective S-boxes that have confusion just as diffusion feature. In [2] proposed for a modified AES algorithm by changing the primary structure where the Mix Columns function was swapped with a Permutation function. Thus, the rounds were overseen by the IP Table obtained from the DES algorithm. The results of their examination displayed that their proposed encryption scheme was rapid while still given the best security. In [3], proposed a Key-Dependent S-box (AES-KDS) to make the AES algorithm more grounded. The encryption and decryption process AES-KDS is like to the original AES cipher as to the number of rounds, information, and key size. Each round capacity in the adjusted structure takes after that of primary AES; however, it is made out of 5 stages as opposed to 4 stages. The extra stage named Rotate S-box displayed close to the start of each round capacity. The other four stages proceed as before. Be that as it may, for the decryption process, there are only 4 stages similar in the original cipher. In any case, the InvSubBytes operation is modified to switch the impact of the Rotate S-box operation recently played out the encryption process. This is followed by a description of key expansion and generation of shift offset-matrix. In [4], the paper effectively advanced the AES calculation by proposing a novel strategy that included Shift Row and S-box changes to outline Mix Column change. This moved closer abstained from the Sub Bytes work. The consequence of their testing S-box indicated that both encryption and unscrambling forms an improvement. In [5], another affiliate S-box affiliate expected to replace the Rijndael S-box. In their paper, they adapted AES coding by setting another stage at the beginning of the circular function. They call the auxiliary stage the name of the S-box rotation that is revised by converting the base S-box as defined by the circular key. The circular key was resolved to utilize the key table algorithm. The spin value depends on the entire circular key. Their examinations demonstrated that the improvement in the essential structural and engineering services did not ignore the security characteristics while providing more confusion without violating the diffusion. In[6], proposed to extend the multifaceted nature and the AES S-box hurried by adjusting the affine transformation and including an affine transformation.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
Eslam wahba afify*, Department of Electrical, Faculty of Engineering, Benha University, Benha, Egypt, eslam.cv@gmail.com
Wageda I. El sobky, Department of Mathematics, Faculty of Engineering, Benha University, Benha, Cairo Egypt, wageda.alsobky@bhit.bu.edu.eg
Abeer Twakol, Department of Electrical, , Faculty of Engineering, Benha University, Benha, Egypt , Abeer.TwakolHYPERLINK "mailto:Abeer.Twakol@bhit.bu.edu.eg"@bhit.bu.edu.eg
Reda Abo Alez, Department of Systems and Computer Engineering Faculty of Engineering, Al Azhar University Cairo, Egypt, profdraboalez@yahoo.com

Performance analysis showed that improvement in cryptographic characteristics of AES S-box. In addition, the number of terms in the enhanced AES S-box algebraic expression had been expanded. Correlation results indicate that the improved AES S-box has better implementation and can be quickly linked to AES.

In [7], presented a novel procedure for the development of S-boxes more than 16 distinctive Galois fields the strategy for linear fractional transformation is embraced by fixing similar parameters for the structure of every box of the 16 S-boxes. The algebraic strength of these recently built S-boxes is measured. All of these S-boxes have nonlinearity the same as AES S-box and hence creating a high level of confusion. In [8], Liu J et al. S-box introduced optimized with all 255 terms in its algebraic expression by switching the linear mapping order and AES primer. In [9], Wang noted that the AES S-box affinity conversion period is 4, and it achieves no more than 16. In [10], Wang et al. consider the structure of AES S-box and draw attention to the fact that the recurring period of AES S-box has a short-term phenomenon, and all periods are less than 88.

In present paper we endeavored to sum up an unordinary cost function created for single yield Boolean functions can be summed up for the instance of S-boxes to deliver significant enhancements for previous work and give their examination based on S-box properties, which are basic for secure S-box development like Non-linearity, Strict Avalanche model (SAC) and Bit autonomy criteria (BIC). Likewise, this improving S-box is contrasted and the AES S-box results.

The structure of the remainder of the paper is as per the following. Section I of this paper displays the Principle of AES S-box generation algorithms. The execution assessment of the powerful S-box against its cryptographic properties is talked about in Section II. Performance Analysis and structure design of the powerful S-box is examined in Section III; Performance comparison presented in Section IV, concludes the research paper represents in Section V.

II. PRINCIPLE OF AES S-BOX GENERATION ALGORITHMS

Rijndael S-box is an array (square set of numbers) used in the AES encryption algorithm. It is working as a lookup table. Substitution is a non-linear transformation that causes bits of confusion. S-box transformation is a non-linear byte substitution, whereby each byte of the state units works independently. The S-box is spoken in the form of a 16 x 16 block, rows, and columns arranged by hexadecimal bits as in the figure. (1). [5].

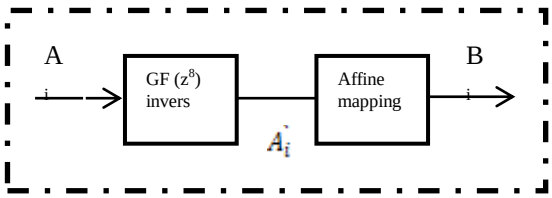

Fig . 1. S-box generation processes [12]

Where $A_i \cdot A_i^{-} = 1$, construction of AES S-box concerning 8 bits as elements in GF (2^8), A AES S-box is a mixture of a power function *f*(*x*) (the multiplicative inverse modulo the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$, which is represented in binary by 0x11b) and an affine transformation *B*(*x*), where.

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

$$S(x) = \begin{bmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{bmatrix} \times f(x) \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \quad (2)$$

Table- I: Coefficient of AES S-box (Hex) [11]

	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

Where the x_is are coefficient of x (i.e., the bits of the bytes), and x_0 is the least significant bit. Thereby, AES S-box can be represented by $S(x) = B \circ f$ An algebraic form is the explanation above, we can develop an expression AES S-box where the coefficients and promoters of algebraic expressions are all in hexadecimal [12].

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

Defenders of algebra are completely isolated into two hex parts detailed in row 1 (m stands for upper bits) and column 1 (denotes lower bits), individually. The remainder of the components are co-ordinations with hexadecimal expressions. In this way, the inverse AES expression is the same as the S-box:

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

From Equation (3), it is certainly not difficult to make the forced expression of AES S-box so simple that only 9 terms are included, while the inverse AES extends S-box 255. The simple algebraic expression of the AES S-box is most prominent and unfavorable. Although there has been no effective violence on this topic yet, a simple algebraic expression is continually seen as an institution for AES cryptanalysis.

III. PROPOSED S-BOX CONSTRUCTION

This section introduces our technology to create a robust 16 x 16 S-box encoded using algebra techniques. It does not care much about any affine transformation matrix and irreducible polynomial is taken. With very low complications, AES S-box safety is expected to be secured. In order to eliminate weak basic algebraic expressions, we are improving the AES S-box. A story structure strategy has been proposed to develop a productive S-box for block ciphers.

In order to get a good performance S-box, we did a lot of tests and simulations.

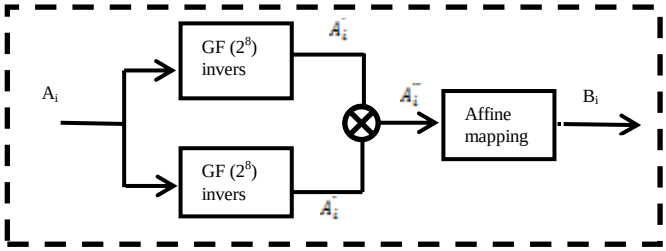

Fig. 2. Power S-box generation processes

The following results can be obtained from simulations: AES S-box Simple algebraic expression is significant to the transformation order of taking multiplicative inverse and applying the affine transformation. The short-term affine transformation period is significant to the selected affine transformation and the short iterative periods are also significant to the selected affine transformation. Therefore, the cryptographic features of the S-box can be improved by modifying the new affine transformation. In our proposed S-box (powerful S-box), we do not change the previous (irreducible polynomial, affine transformation matrix and affine constant), but the complexity of the algebraic expression increments with the capacity to oppose against differential cryptanalysis unaffected. The powerful S-box optimization scheme is created by the following three steps:

Step 1: Taking multiplicative inverse:

$$S(x) = \begin{cases} (x^{-1}), & x \neq 0 \\ 0, & x = 0 \end{cases} \quad (5)$$

Step 2: Taking multiplicative inverse again:

$$S''(x) = S(x)^{-1} = \begin{cases} s(x)^{254} & x \neq 0 \\ 0, & x = 0 \end{cases} \quad (6)$$

Step 3: Applying the affine transformation L8F; 63.

$$S''(x) = \begin{bmatrix} 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \\ 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \end{bmatrix} \times S(x)^{-1} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \quad (7)$$

Table- II: Coefficient of the powerful S-box (Hex)

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

IV. RESULT AND DISCUSSION

Performance Analysis of the powerful S-box The power of block ciphers, which work to replace and permutation as strongly as AES, depends on the construction of the S-box (the first layer of the AES system) which must fulfill some basic properties to build up a safe cryptosystem, that could resist algebraic attacks. Then, we detail and Present the performance analysis of our powerful S-box (Powerful S-box). We construct S-box using MATLAB. And then, we make the performance analysis of the S-boxes.
The S-box takes to throw the following tests.

A. Balance

A Boolean function is said to be balanced whenever the yield vector has an equal number of zeros and ones. A Boolean function is said to be balanced in the event that it meets a condition formulated where n is a Boolean variable and HW is Hamming weight, which is the number of ones in the truth table of f(x). In otherworld, $f(x), \{x \mid f(x) = 0\} = \{x \mid f(x) = 1\}$. For this situation, when n= 8 then$HW\ (f(x)) = 128$. Therefore, it accepts the balance criterion for a powerful S-box [13].

$$hwf((x)) = \sum_{x=0}^{2n-1} f(x) = 2^{n-1} \quad (8)$$

B. Bijective

Requires a one-to-one and onto mapping from input vectors to yield vectors. An $n \times n$ S-box is bijective if each yield produces an unlike value and is in the interval $(0, 2n-1)$. The powerful S-box has diverse yield values table 2 in the interval (0, 255). Along these lines, it accepts the bijective criterion for a powerful S-box [14].

C. Strict avalanche (SAC)

It happens if some information bit (i) is modified; each portion of the return will change with an average possibility. A strict avalanche requires that in the event of trivial changes to the income conductor, there will be an important modification in the performance conveyor. To reach this result, we will need a function that is sure of on 50% of each of its (n) input bits.
Although each performance bit function in Power S-box cannot meet SAC; however, the amount of variable performance bits is exceptionally close to$2n - 1 = 128$, that is, it is possible to approach 1/2. When a portion of the input bit is reversed, its peak performance is reversed compared to the possibility to approach near 1/2. The result of the analysis powerful S-box shown in table (3).The judgment of overall SAC analysis of proposed Powerful S-box and other AES S-boxes is presented in Tables (4). The results of the powerful S-box analysis are given in Table (3). A comprehensive comparison of the SAC analysis of the proposed Powerful S-box and other AES S-boxes is shown in Table (4).

Table- III: SAC of Powerful S-box

SAC	*f1*	*f2*	*f3*	*f4*	*f5*	*f6*	*f7*	*f8*
1	116	120	140	124	116	124	116	124
2	140	132	128	120	124	132	136	132

4	128	124	124	124	136	116	124	116
8	124	124	124	116	140	120	120	124
16	124	120	120	120	124	120	120	136
32	120	140	128	128	124	116	128	140
64	128	136	128	112	120	128	132	124
128	128	116	124	140	112	140	124	124

Table- IV: SAC of S-boxes

S-boxes	Powerful	APA	Gray	AES	Ref.[8]
SAC	0.494	0.510	0.476	0.504	0.487

D. Bit independence

BIC requires that the yield bits be produced independently of each other. In other words, there should not be any statistical pattern or statistical dependencies between the yield bits of the yield vector. The elite or two bits of S-box must be very nonlinear. Consequently, the distinguishing characteristic of BIC is its non-linear (BIC-nonlinearity) performance shown in Table (5). Therefore, the average nonlinearity BIC is 112.

Table- V: BIC of S-box.

S-boxes	Powerful	APA	Gray	AES	Ref.[8]
BIC	112	112	112	112	112

E. Nonlinearity

Necessitates that S-box is a nonlinear mapping from input to yield. This would make the cryptosystem vulnerable to attacks. On the off chance that the S-box is created with maximally nonlinear Boolean functions, it will give a bad calculation by linear functions as a result of making a cryptosystem difficult to break. Let $a \cdot x^2 + e$ be the new arrangement of all Boolean functions where $a \in F_2^n$ and $e \in F_2$. Also, let $b.F = b_1f_1 + b_2f_2 + \cdots + b_mf_m$ be a linear grouping of the coordinate Boolean functions f_1 of F where $b = (b_1;, b_2, \ldots\ldots, b_m) \in F_2^m$ is nonzero. The nonlinearity (NL) for an S-box is defined as.

$$NL(f(x)) = min\, d(f(x), g(x)) \qquad (9)$$

The nonlinearity of an $n \times n$ S-box is the lowest Hamming Distance among the arrangement of all non-constant linear groupings of element functions of F and the arrangement of all affine functions over F_2^n. Clearly recommended that NL must be near to the well-known nonlinearity, (i.e., *NL* = 112 obtained by AES S-box) to obstruct linear cryptanalysis[15].

Therefore, Thusly, in this paper, we set *NL*>100 for an S-box to be characterized as cryptographically strong. In this paper, we think about linear combinations between coordinate functions, which make the estimation of the NL of an S-box stronger and stricter. Non-linearity of recently recommended an S-box is 112 and an examination is made with some exemplary also, as of late built S-boxes is shown in Table (6).

Table- VI: Nonlinearity analysis of S-boxes.

S-boxes	Powerful	APA	Gray	AES	Ref.[8]
Average NL	112	112	112	112	112

F.Differential uniformity.

The minimum differential homogeneity is: $\delta(S) = 2n - m + 1$ for an n × n S-box that is called an Almost Perfect Nonlinear (APN) S-box. Of course, there is no APN S-box in GF (2^n) if *n* is even. Thereby, for the enhanced AES S-box, n =8, δ= 4. We compute the differential circulating matrix $\Lambda(S)$, in the outcome, the differential homogeneity of the improved AES S-box is: with the exception of component λ_{00}, the estimation of different elements is just 0, 2, or 4, besides, there is just a single 4 in each row and column and that the diffusion of 0 and 2 does not change. It is clear that the Powerful S-box is differential homogeneity, which can resist against differential cryptanalysis well.

For a correlation, the cryptographic properties of different AES S-boxes and the proposed Powerful S-box are tested by experiments and simulations. The results of the performance comparison are presented in Table (7). As shown in Table (7), the DSAC of our proposed S-box is reduced from 432 to 372. That is, the Powerful S-box has a better performance in SAC than AES S-box and the APA S-box [16]. The affine transformation period is expanded from (4, 16) to 102, so our proposed S-box has an excellent performance in affine transformation over AES S-box and the APA S-box. The iterative period of the improved AES S-box is expanded to 256, while the iterative periods of AES S-box and the APA S-box are less than 88. To put it plainly, the Powerful S-box has better cryptographic properties. By replacing AES S-box with the Powerful S-box, it very well may be effectively applied to AES. Simulations suggest that the Powerful S-box works efficiently in AES.

Table- VII: Cryptographic properties comparisons of S-boxes

Performance index	***Optimal value***	***AES***	***APA***	**Ref.[8]**	***Gray***	***Powerful S-box***
Balance criteria	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Bijective	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
SAC	*0.5*	*0.504*	*0.510*	*0.508*	*0.476*	*0.494*
Bit independence	*112*	*112*	*112*	*112*	*112*	*112*
Non linearity N(F)	*112*	*112*	*112*	*112*	*112*	*112*

Differential uniformity $\delta(F)$	*4*	*4*	*4*	*4*	*4*	*4*
Affine transformation period	*increase*	*4*	*4*	*16*	*16*	*102*

From the above correlation, it is clear that Performance analysis of our new affine powerful S-box satisfies the most required S-box criteria and benchmarks, similar to SAC, BIC, NL, and so on. Let's compare the cryptographic characteristics of the powerful S-box with other AES S-box as shown in Table (7). One of the contributions of this paper is listed boldly in Table (7). With the structure proposed in this paper, the algebraic complexity of the powerful S-box is increased by increasing the affine transformation period from 4, 16 to be 102 in our powerful S-box, and other S-box criteria performance analysis is better.

V. CONCLUSIONS

This paper proposed another change and prescribed a novel technique to build great S-boxes utilizing the algebraic method. The security strength of the proposed (powerful S-box) was inspected utilizing different standard criteria. The simulation results according to other noteworthy as per other significant S-boxes, legitimizing the execution of our S-box method. The performance of our powerful S-box was great in the majority of the situations when compared with other modern S-boxes. In particular, the scores of the SAC, BIC, non-linearity, DP, and Affine transformation period of The promising aftereffects of the powerful S-box examination make it a potential possibility for use in cutting edge S-box design domain. It is worth mentioning that our method is the first to explore the affine transformation for S-box construction. Stronger S-boxes using powerful transformation methods, like the proposed powerful S-box, are expected to emerge for usage in practical systems for secure communication.

REFERENCES

1. A. R. Abd-ElGhafar, A. Diaa, and F. Mohammed, "Generation of AES key-dependent S-boxes using RC4 algorithm," in 13th International Conference on Aerospace Sciences & Aviation Technology, 2009, pp. 26-28.
2. P. Kawle, A. Hiwase, G. Bagde, E. Tekam, and R. Kalbande, "Modified Advanced Encryption Standard," International Journal of Soft Computing and Engineering (IJSCE), vol. 4, 2014.
3. G. Krishnamurthy and V. Ramaswamy, "Making AES stronger: AES with key-dependent S-box," IJCSNS International Journal of Computer Science and Network Security, vol. 8, pp. 388-398, 2008.
4. R. Riyaldhi and A. Kurniawan, "Improvement of advanced encryption standard algorithm with shift row and S. box modification mapping in mix column," Procedia computer science, vol. 116, pp. 401-407, 2017.
5. J. J. R. M. S. Sulaiman and J. Ramli, "Enhancing advanced encryption standard S-box generation based on round key," International Journal of Cyber-Security and Digital Forensics (IJCSDF), vol. 1, pp. 183-188, 2012.
6. J. Cui, L. Huang, H. Zhong, C. Chang, and W. Yang, "An improved AES S-Box and its performance analysis," International Journal of Innovative Computing, Information, and Control, vol. 7, pp. 2291-2302, 2011.
7. T. Shah and D. Shah, "Construction of highly nonlinear S-boxes for degree 8 primitive irreducible polynomials over ℤ 2," Multimedia Tools and Applications, vol. 78, pp. 1219-1234, 2019.
8. L. H. J. CUI, H. ZHONG, C. CHANG AND W. YANG, "AN IMPROVED AES S-BOX AND ITS PERFORMANCE ANALYSIS," International Journal of Innovative Computing, Information and Control vol. 7, 2011.
9. Y. B. Wang, "Property of affine transformation in S-box of AES," PLA University: Science and Technology, vol. 4, p. 9, 2002.
10. Y. B. Wang, "Analysis of structure of AES and its S-box," PLA University: Science and Technology, vol. 3, p. 5, 2002.
11. I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, "S 8 affine-power-affine S-boxes and their applications," Neural Computing and Applications, vol. 21, pp. 377-383, 2012.
12. J. Daemen and V. Rijmen, 1999., "AES Proposal: Rijndael, http://www.east.kuleuven.ac.be/ ~rijmen/rijndael," 1999.[13]H. I. Shah T, Gondal MA, Mahmood H "Statistical analysis of S-box in image encryption applications based on majority logic criterion," Int J Phys Sci 6, vol. 16, p. 17, 2011.
13. A. Y. Razaq, A.; Shuaib, U.; Siddiqui, N.; Ullah, A.; Waheed, A., "A Novel Construction of Substitution Box involving Coset Diagram and a Bijective Map," Secur. Comm. Netw, 2017.
14. Y. Naseer, T. Shah, D. Shah, and S. Hussain, "A Novel Algorithm of Constructing Highly Nonlinear Sp-boxes," Cryptography, vol. 3, p. 6, 2019.
15. L. Cui and Y. Cao, "A new S-box structure named Affine-Power-Affine," International Journal of Innovative Computing, Information and Control, vol. 3, pp. 751-759, 200

AUTHORS PROFILE

Eng.Eslam wahba afify, He received his MSc degree in Electrical Engineering in 2015, at the Department of Electrical, Faculty of Engineering, Benha University, Benha. He is currently with the Department of Electrical as a Ph.D. student. He is interested in the subjects of digital image processing, network security, and cryptography techniques.

Dr. Wageda I. El sobky, She received his MSc degree in applied mathematics from Benha University in 2012; she received a Ph.D. degree in applied mathematics Ain Shams University, in 2017. She is currently a doctor in basic engineering sciences at the Faculty of Engineering, Benha University. She is interested in the subjects of information security and cryptography techniques.

Dr. Abeer T. Khalil: She received a Ph.D. degree in Electrical Engineering, at the electronics and communications engineering department, faculty of engineering at mansoura University. She is currently an assistant professor at the faculty of engineering Benham University. She is interested in the subjects of wireless networking and hardware realizations of digital systems.

Prof. Dr. Reda Abo Alez: He is currently a prof. doctor in Systems and Computer Engineering at Faculty of Engineering, Al Azhar University Cairo, Egypt. He is interested in the subjects of Annotation System, information security and cryptography.