Performance Analysis of Advanced Encryption Standard (AES) S-boxes

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

Abstract : The Advanced Encryption Standard (AES) algorithm is available in a wide scope of encryption packages and is the single straightforwardly accessible cipher insisted by the National Security Agency (NSA), The Rijndael S-box is a substitution box S-Box assumes a significant job in the AES algorithm security. The quality of S-Box relies upon the plan and mathematical developments. Our paper gives an outline of AES S-Box investigation, the paper finds that algebraic attack is the most security gap of AES S-Box, likewise give a thought regarding distinctive past research to improve the static S-confines that has been utilized AES, to upgrade the quality of AES Performance by shocking the best S-box.

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

I. INTRODUCTION

All encryption algorithms affirmed by the NSA for ordered handling were, characterized. The quality of any great encryption algorithm is not improved by holding the plan as a mystery. An open space encryption standard is dependent upon consistent, expert cryptanalysis. Any leaps forward will probably be accessible to clients and their foes in the meantime [1]. **DES** (Data Encryption Standard) and AES both are the symmetric block cipher. AES knew about beat the weight of DES. As DES has a more minor key size which makes it less secure to beat this triple DES was natural yet it winds up being slower. Along these lines, later AES was presented by the NIST. The basic complexity among DES and AES is that in DES plaintext square is isolated into two halves before the primary calculation starts to begin while in AES the whole square is set up to get the ciphertext. By inspects some more differentiation among DES and AES. DES is the more established calculation and AES is the propelled calculation that is quicker and more secure than DES. So what is AES? In August 2000, the Belgian block cipher "Rijndael" was picked as a champ to be the AES [2]. This happened remarkably an open test with worldwide collaboration was held by the NIST of the United States to find a successor for the 24-year old the DES. Rijndael is a key-iterated block cipher with an astoundingly rich and strong arithmetical structure. The square and key lengths are variable in adventures of 32 bits in the region of 128 and 256 bits. The fundamental genuine data square length for AES is 128 bits that as it might; the key length for AES possibly 128, 192, or 256 bits [2, 3]. The conversation is focused on Rijndael S-Box yet a huge amount of the trade can in like manner be associated with the ideal security of block cipher and the objective of the cryptanalysis. As follows the paper is sorted out: Section II gives a detailed analysis of the structure of the AES. Section III scope in the cryptanalysis study of algebraic techniques against block ciphers, gives a detailed analysis of S-Box algebraic structure and characteristics of algebraic resisting attack. Section IV presents the previous researchers developed on S-Box constructions. Conclusion remarks in Section V.

Manuscript received on April 02, 2020.
Revised Manuscript received on April 20, 2020.
Manuscript published on May 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

II. AES GENERATION ALGORITHMS

The AES is the Repetitive aversion Feistel cipher [4]. It’s depended upon 'substitution–arrange to sort out'. It joins a development of related activities, a variety of which fuse uprooting responsibilities by express yields (substitutions) et al fuse improving bits around. Curiously, AES play out the blend of its estimations on bytes as opposed to bits. During this design, AES treat 128 bits of a plaintext deter as sixty bytes. These sixty bytes are filtered through in 4 portions and 4 sections for getting ready as a cross-zone Unlike DES, [5]. The plan of the AES organization is given within the going with a portrayal plaintext that treated as a byte framework of size 4 x 4, where each byte addresses a remarkable force in GF (2^8). An AES round applies four exercises to the state cross-section [2].

A. *Sub Bytes*

The information 16 bytes are switched by investigating an immovable table S - confine given plan. The result could be a system of four row and four segments.

B. *Shift Rows*

Every line of the four lines of the cross section is moved to the other side. Any information sources that 'tumble off' are re-embedded on the right half of the line [3].

A. *Mix Columns*

Each area of 4 bytes is at the present changed utilizing a vital numerical edge. This edge takes as data the four bytes of 1 area what's more, yields four new bytes, which override the focal piece.

The result is another new structure containing 16 new bytes. It should be seen that this headway isn't acted inside the last round [4].

B. Add Round Key

The 16 bytes of the structure are beginning at now considered as 128 bits and are XOR to the 128 bits of the round key. Just if this can be the last round, by then, the yield is the ciphertext. Something different, the going with 128 bits are deciphered as 16 bytes and that we start another relative round [5].

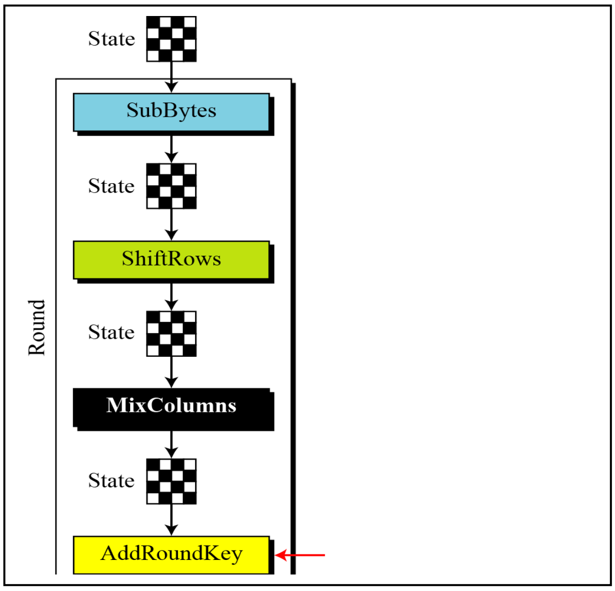


Fig.1. (A) AES one round structure. (B) AES structure [3].

III. THE S-BOX GENERATION THEORY

The S-Box (replacement Box) is an essential portion of lopsided key calculations that play out the replacement. In square figure; they're conventionally acquainted with obscure the association between the key and in this manner the figure message Shannon's property of disorder. At the point when everything is asserted in done, any s-box takes some number of data bits (*m*) and changes them into some number of yield bits (*n*), where (*n*) isn't identical to (*m*). S-confine is additionally made two, unquestionable propensities: Static and Dynamic. In Static S-box, input vector regards aren't changed while in Dynamic S-box input vector regard changes. Following the Static and Dynamic view.

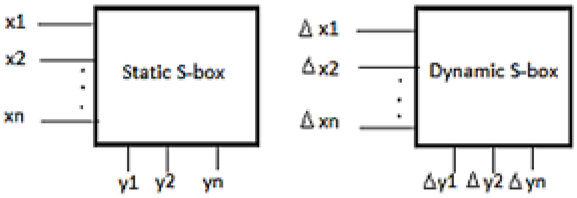


Fig.2. Dynamic & Static S-Box [4].

Static and dynamic S-box properties were characterized utilizing fig 2. A measurement to gauge the irregularity of information is entropy characterized by H (*Z*) for arbitrary variable "z" as follows: High entropy suggests hard calculating the characteristics. S-box should satisfy better entropy regards. The Rijndael S-Box (replacement box) [6] is a system (square show of numbers) used in the (AES) cryptographic computation. Is fills in as an inquiry table.

Replacement is a nonlinear change that performs confusion of bits. S-Box is addressed as a 16x16 display, lines, and segments requested by hexadecimal bits [7].

A structure of AES S-Box viewing 8 bits as components in GF (2^8), AES S-Box is a mix of a force work *f(x)* $x^8+x^4+x^3+x+1$ (the multiplicative converse modulo the unchangeable which is signified in double by 0x11b) and a relative change 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 (the least significant bit. From the above portrayal, we can infer the AES S-Box arithmetical articulation [7]:

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

The coefficients and kinds of scientific explanations are all in hexadecimal. The coefficients of the scientific explanation of the AES in reverse S limit are shown in the table (1). The types of mathematical articulation are separated into two sections in hexadecimal that are recorded in segment 1 (*m* signifies the upper bits) and column 1 (*n* indicates the lower bits), individually [9, 10]. The remainder of the climate in Table 2 is coefficients relating to the types of mathematical articulation in hexadecimal. Subsequently, the mathematical articulation of AES opposite S-Box is indistinguishable to:

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

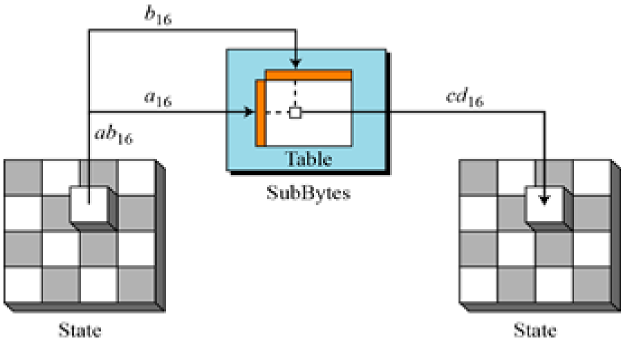


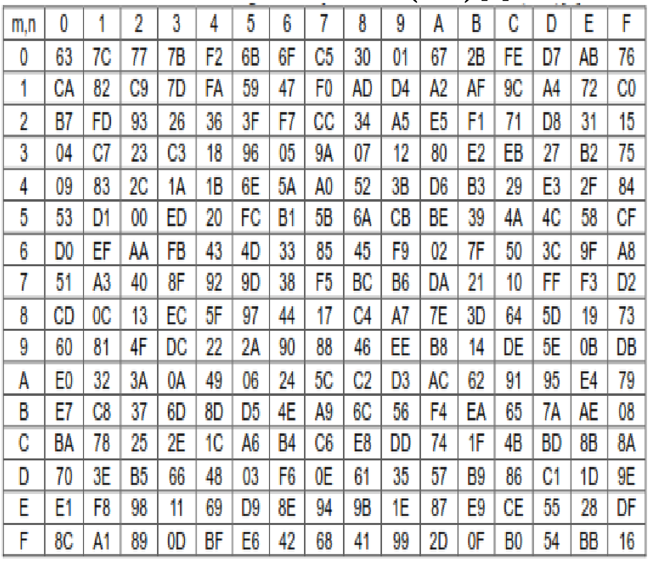
Fig.3. SubBytes and InvSubBytes processes [3]

From Equation (3) and Table (1), it is not hard to get that the logarithmic verbalization of AES S-Box is anything but difficult to the point that singular 9 terms are incorporated, while the AES switch S-Box shows up at 255.

The focal logarithmic enunciation of AES S-Box is the head charming and disadvantageous properties the away from clarification of AES S-Box is the chief hypnotizing and disadvantageous properties.

However no old trap has been found about it up to now, the unmistakable logarithmic verbalization is dependably observed because of the establishment for cryptanalysis AES. The standards and modules are gotten by many square figures since Rijndael was picked as AES. We call this sort of S boxes AES-like [8].

Table1. The AES S-Box (Hex) [2]



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

A. Algebraic property of s-box

One S-Box with fantastic cryptographic properties can guarantee the figure to limit against a gathering of cryptanalysis methodologies, so any insufficiencies of S-Box will disable the security of the figure [10]. AES S-Box is a 8×8 Boolean cutoff, and these 8 Boolean cutoff points condition and affect one another. Regardless of whether these 8 cutoff points have several properties simultaneously, the S-Box Boolean breaking point may have not for all intents and purposes indistinguishable properties [9] Therefore, it is basic to eviscerate the arithmetical properties of the S-Box work.

B. Algebraic cryptanalysis of S-box

The objective of logarithmic cryptanalysis is to break cryptosystems by utilizing numerical instruments originating from the representative calculation and current polynomial math [11]. Significantly more successfully, an arithmetical snare can be separated in two phases: first, the cryptosystem and its focal centers must be changed over into a tremendous measure of multivariate polynomial conditions, second, the blueprints of the acquired polynomial framework must be figured. The security of cryptographic grungy therefore emphatically depends upon the trouble of understanding the related polynomial framework.

These ambushes have been wound up being extremely valuable for both open key or symmetric cryptosystems; square and stream figures. Since productive Gröbner premise attacks on square and stream figures are conceivable, it must be thought about unequivocally how Gröbner premise computations depend upon the structure of polynomial systems identifying with square and stream figures. One of the potential methodologies depends on the documentation of semi-customary arrangements of polynomials one of the possible approaches relies upon the documentation of semi-typical groupings of polynomials [7, 8]. Utilizing the AES as a model, we have estimated three mathematical portrayals for block ciphers. It was demonstrated that the AES polynomial conditions over GF (2^8) are not semi-normal and that the AES frameworks of quadratic conditions (QM) over GF (2) are not semi-ordinary over GF (2).

Definition3. [10] Given Γ conditions of t terms in GF (2^8), the obstruction of arithmetical assaults (RAA) s signified by Γ and is characterized to

$$\Gamma = \left({}^{(t-r)} \Big/ {}_{n}\right)^{\left({}^{(t-r)}/{}_{n}\right)} \qquad (5)$$

Be For AES S-box, t = 81, r = 23, n=8, we can get Γ≈222.9. Jung [11] asserted (Γ) ought to be more noteworthy than 232 for secure figures. While AES S-Box has Γ=222.9, it tends to be a shortcoming of AES.

Note: These measures depend generally after taking a multiplicative opposite. For the improved AES S-box, we can obtain Γ=222.9.

Note: Any S-Box where each yield is made by a wound limit of information bits, and where any immediate blend of the yield bits is moreover a bowed capacity of the information bits, is additionally a perfect S-Box

IV. RESULT AND DISCUSSION

Past specialists built up a few S-Box developments which will be talked about in the accompanying lines by thinking about the extent of arithmetical assaults.

A. Alamsyah et al. [10]

Presented a novel S-Box that uses one polynomial m(x) = $x^8+x^6+x^5+x+1$ with an additional fixed 8 bites (00000001). The nature of the S-Box took her to the sword in the use of balance, bijective, nonlinearity, SAC, and (BIC-nonlinearity). Final test results show that the S-Box was balanced and was bijective. The tests also gave the standard nonlinearity of 112, the ordinary SAC of 0.4995, and thus the normal nonlinearity of BIC 112. These results exhibit that the proposed S-Box had a prevalent security level that stood out from other existing S-boxes.

B. Wei Yang et al [11]

Exhibited that by including a relative change before multiple conversations, the idea is multifaceted for both the scientific pronouncements of AES S-Box, and thus, improves the logarithmic formulation of the back S-Box. The terminology measurement in AES S-Box scientific vocabulary ranges from 9 to 255, so the amount of terms in the digital pronunciation of the S-Box conversation ranges from 9 to 253. In this way, only 9 terms in AES S - the logarithmic of the fund’s dialect, thus the opposite numerical interpretation of the S-Box can get away from its hands.

Retrieval Number: F9712038620/2020©BEIESP
DOI:10.35940/ijrte.F9712.059120
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

C. Wang and Liu [12]

They suggested improving the S-Box by exchanging a cross-punching request and applying the relevant change. The numerical form of the S-Box includes 255 terms and its hash in the SAC is 408. However, since this process must have some drawbacks, for example, the logarithmic pronunciation of the corresponding S-Box only includes 9 terms. The numerical pronunciation of the corresponding S-box is very direct. Likewise, the related change period 4 is still and its recurring period is less than 88. S-Box has similar encoding properties with AES S box.

D. Gupta and Sarkar [13]

Acquainted two new procedures with structure non-straight adaptable S-boxes and exhibited that the association opposition of the adaptable S-boxes is protected under a course of action with an optional Boolean limit. Regardless, their approach wasn't strong to the logarithmic ambushes.

E. Fahmy et al. [14]

Familiar with the S-Box key production strategy specifically for AES, which can be done from the secret key with the help of two parameters for direct coordination of ISO-C standard and GNU-C separately. They also tried to calculate the mediation rating and found excellent results. Regardless, they replaced their unique S-Box operation with the new stunning S Box and got tired of the inverted S-box, which was a complete violation of the AES structure.

F. Janadi & Tarah [16]

Expressed that AES was intended to oppose probabilistic assaults however is progressively appropriate to logarithmic assaults after the exposure of XSL (broaden end Sparse Linearization) assault. Along these lines, they proposed an alteration in the age of S-boxes by blending each estimation of the static S-Box with a worth created by MD5 (Message Digest) hash work. They have likewise tried their proposition utilizing factual tests and presumed that their calculation doesn't disregard any security certifications.

So our article plan most research offers that had been finished by the scientist by years, this content chooses three styles of the preeminent force S-Box that improved upheld the arithmetical structure [1, 9, 12]. to frame the correlation, the cryptographic properties of AES S-Box, and the improved AES S-Box are examinations [1, 9, and 12]. Execution correlation results are given in Table (2).

As often shown in Table 2, the Strict Avalanche Effect DSAC model of the enhanced AES S box is reduced. This means that the enhanced AES S-Box includes a dominant introduction to the Strict Avalanche Effect (SAC) hypothesis from AES S-Box and S-Box Affine-Power-Affine (APA).

The amount of terms is increasing in the AES S-Box enhanced digital joint accessory. In addition, the enhanced AES in the S-Box Reverse Sports Joint includes an unlimited number of terms from the A-box AES key. Basically it can maintain a vital good way out of just 9 weaknesses in the AES S-Box digital hinge as well as in the S-Box Affine-Power-Affine (APA) logical component. The related change period has been extended; the enhanced AES S-Box has an optimal implementation of proportional change compared to AES S-Box in addition to the S-Box (APA).

Table2. Comparisons of S-boxes cryptographic properties [9]

Performance index	AES S-box[1]	Affine-Power-Affine [12]	Improved S-box[9]
Balance criteria	balance	balance	balance
Differential uniformity$\delta(F)$	4	4	4
Non-zero linear structure	none	none	none
The resistance of algebraic attacks r	$2^{22:9}$	$2^{22:9}$	$2^{22:9}$
Distance to SAC	432	408	372
Nonlinearity 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

The recurring time for an enhanced AES fund is extended. Honestly, the improved AES S-Box has better encryption features. By registering in AES S-Box with enhanced AES S Box, all the right things can also be used in AES. The paper notes that the complexity of the principle of construction and forced expression of the S-Box design are beneficial for improving AES safety versus an algebra attack.

V. 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 a complete study and scopes three types of existing S-Box by performance analysis and comparative Performance study as can be seen from the table (2). By research and study analysis, the paper finds that algebraic attack is the 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, the S-Box equation system must have strong (RAA).

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 (AES) resist 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, Affin 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. 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.

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.