INTERNATIONAL JOURNAL OF Telecommunications
AIR DEFENSE COLLEGE

Design and Implementation of Advanced Encryption Standard by New Substitution Box in Galois Field (2^8)

Wageda Al-Sobky [1], Abdelkader Ismail [2,*], Ashraf Mohra [3], Ayman Hassan[4], and Ayman Abdelaziem [5]

Citation: Al-Sobky, W.; Ismail, A.; Mohra, A.; Hassan, A.; Abdelaziem, A. *International Journal of Telecommunications, **IJT'2022**, Vol. 02, Issue 01, pp. 1-11, January 2022.* https://ijt-adc.org/articles/2805-3044/647531

Editor-in-Chief: Yasser M. Madany

Academic Editor: Youssef Fayad

Received: 18-11-2021
Accepted: 25-12-2021
Published: 1-1-2022

Publisher's Note: The International Journal of Telecommunications, IJT, stays neutral regarding jurisdictional claims in published maps and institutional affiliations.

[1] Department of Basic Sciences, Benha Faculty of Engineering, Egypt.; wageda.alsobky@bhit.bu.edu.eg
[2] Electrical Engineering Department, Benha Faculty of Engineering, Egypt; Abdelkader0kita@gmail.com
[3] Electrical Engineering Department, Benha Faculty of Engineering, Egypt; amohra@bhit.bu.edu.eg
[4] Electrical Engineering Department, Benha Faculty of Engineering, Egypt;ayman.mohamed@bhit.bu.edu.eg
[5] Computer Engineering Department, October University, Egypt; ayman.hasanein@o6u.edu.eg
* Correspondence: ; Abdelkader0kita@gmail.com

Abstract: An inverse multiplexing method for irreducible polynomials is presented in this paper based on the theory of substitution boxes. The method is based on the theory of substitution boxes. Following a series of successful experiments, the new approach was put into practice. For reasons of increased complexity and security, the affine conversion period in the Galois field (2^8) has been increased to the maximum value of the period between input and output of 102, the Strict Avalanche Criterion (SAC) has been reduced to nearly half of its original value, and the results are bijective as a result. It was decided to use the number 112 after the Bit Independent Criterion effect had been reduced to produce good results. These breakthroughs are being used to protect information security and to strengthen the advanced encryption standard that is currently in use, according to the researchers. In addition to the addition of a new s-box, their encryption will be more secure and private, making our services even more valuable.

Keywords: S-Box, Bit independence, Advanced Encryption Standard, Galois Field, Bijective, Balance, SAC.

1. Introduction

Before the advanced encryption standard (AES), one more encryption standard called the information encryption standard (DES) was created by IBM and normalized by the US National Bureau of guidelines. The framework was presented in 1970 and served the web world for over twenty years until security specialists acknowledged during the 1990s that this encryption standard was helpless against hacking and information spillage [1]. The security weakness of the DES standard was evident to the public when the moral hacking association freely hacked DES in under 24 hours. That denoted the finish of over twenty years of the strength of the DES standard as a standard encryption convention [2]. It was required five years after this occasion acknowledgment model advanced standard encryption, this time took complex calculations. However, we should summarize the story here to discover the underlying data. [3]. Because of all the above mentioned, DES was presently not a standard encryption framework. The National Institute of Standards and Technology looked for encryption models created by all influential organizations on the planet at that point, including IBM, towfish, Rijndael, RSA Security [3]. The assessment cycle for each plan was exhaustive and exact, including Real-Time Attack appraisals, conversations and contentions, and quality tests. Furthermore, following five years of thorough testing strategies, and solely after that, Rijndael was picked as the best crypto standard among its rivals. Rijndael was subsequently renamed AES after normalization [4]. AES activity is based on principles called code blocks. The work of AES mainly involves the development of tasks such as exchange and replacement [5]. A key is a code utilized by the

AES standard to encode information and decrypt encrypted data. AES has three main sizes: 128-bit, 192-bit, and 256-bit. There are ten rounds,12 rounds, and 14 rounds [6]. The National Institute of Standards and Technology (NIST) announced a call for proposals. For Advanced Encryption Standard (AES) [7]. Twenty-one recommendations, fifteen of which were approved after two years of public consultation and research were reduced to five finalists for further analysis. Rijndael won the contest and was elected in October 2000 [8]. The AES block size is 128 bits and supports 128, 192, and 256-bit key sizes. The number of rounds is 10, 12, or 14 sizes, and each of the three keys is different as DES and AES Expected to attract much attention from cryptanalysts [8].
This paper will provide a new design method of the s-box that gives good results and will be used for other ways to implement advanced encryption standards developed. Analyze several tests that prove the new s-box strength, compare the results with other researchers, and implement the encryption standard using FPGA.

2. The Operation of the Inverse S-box

Taking multiplicative inverse (x) in GF (2^8) (x)-1) is defined by

$$\mathrm{Inv}(x)=\begin{cases} (x)^{254} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

$$\begin{bmatrix} C0 \\ C1 \\ C2 \\ C3 \\ C4 \\ C5 \\ C6 \\ C7 \end{bmatrix} = \begin{bmatrix} 0,0,1,0,0,1,0,1 \\ 1,0,0,1,0,0,1,0 \\ 0,1,0,0,1,0,0,1 \\ 1,0,1,0,0,1,0,0 \\ 0,1,0,1,0,0,1,0 \\ 0,0,1,\ 0,1,\ 0,0,1 \\ 1,0,0,1,\ 0,1,0,0 \\ 0,1,0,0,1,\ 0,1,0 \end{bmatrix} \begin{bmatrix} S\text{-}BOX0 \\ S\text{-}BOX1 \\ S\text{-}BOX2 \\ S\text{-}BOX3 \\ S\text{-}BOX4 \\ S\text{-}BOX5 \\ S\text{-}BOX6 \\ S\text{-}BOX7 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad (1)$$

Multiplying the coefficients of polynomial equations to find the inverse result of the 255 bits to be used in the Galois field, Equation (1) shows how to find the inverse of the s-box. The inverse affine transformation also represents the sum of multiple rotations of the byte as a vector, where addition is the XOR operation [9]. Necessary inverse multiplication in the irreducible polynomial shows a nonlinear system whose results are difficult to predict.

Table 1. The Substitution box inverse.

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

Using Table (1) and polynomial, we get 255 bits. All of these are based on nonlinear theories and asymmetric numbers that are difficult to predict.

3. The S-box Principle of Operation

Rijndael Cipher (AES) is applied in various situations and applications where data and information need to be protected. Non-linear replacement operations are a significant factor in the strength of AES encryption systems. The S-Box component used by AES is fixed and cannot be modified. The proposed approach aims to use a double key in the encryption and decryption process of the Sub Byte conversion function. The first key will generate some random S-boxes, depending on the use of multiple keys that lead to S-boxes' generation. However, suppose each has a reversely assigned S-box. In that case, the second key is a random distribution of the S-box, and the two keys. This poses some problems as the delay during the Encryption and the reverse operation process of the sub byte function. In comparison with other techniques, this method has the advantage of having outstanding performance, cryptographic strength, and resistance to linear and differential cryptanalysis. The box next to the cryptographic key must be known [10]. Equation (2) shows the way to find the S- box.

$$S\text{-}BOX=[MATRIX\ (G)\times (x\text{-}1+\ C\ )] \tag{2}$$

MATRIX (G)=1F C=63 X=Inverse table

$$\begin{bmatrix} S\text{-}BOX7 \\ S\text{-}BOX6 \\ S\text{-}BOX5 \\ S\text{-}BOX4 \\ S\text{-}BOX3 \\ S\text{-}BOX2 \\ S\text{-}BOX1 \\ S\text{-}BOX0 \end{bmatrix} =[MATRIX\ G] \begin{bmatrix} 1,1,0,0,1,1,1\ ,1 \\ 1,1,1,\ 0,0,1,1,1 \\ 1,1,1,1,0\ 0,1,1 \\ 1,1,1,1,0,0,0,1 \\ 1,1,1,1,1,0,\ 0,0 \\ 0,1,1,1,1,1,0,0 \\ 0,1,1,1,1,1,1,0 \\ 0,0,0,1,1,1,1,1 \end{bmatrix} \begin{bmatrix} C0 \\ C1 \\ C2 \\ C3 \\ C4 \\ C5 \\ C6 \\ C7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Table 2. The S-box.

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

4. Proceedings of Advanced Encryption Standard.

The main distinction between DES and AES is that the squares in the plaintext are divided into two halves before the linear computation begins in DES. While on the other hand, the AES is separated before starting the linear analysis [11]. A closer look reveals the distinction between DES and AES. Advanced encryption standard is non-linear calculation and complex calculation So, it is safer and faster than DES So what are the AES procedures?

4.1 Initial operation

The first round of AES encryption includes an (exclusive or) process for the encryption key with plain text Figure 1, shows the primary process.

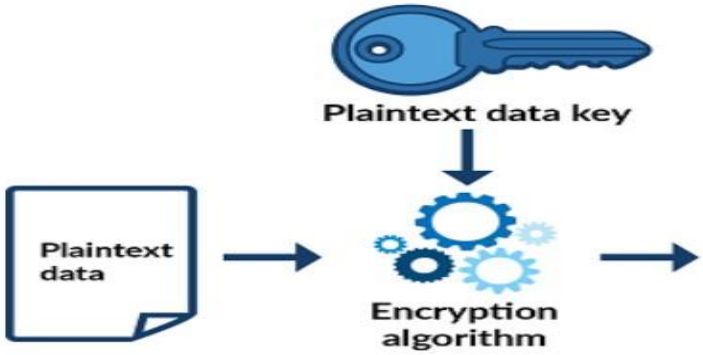

Figure 1. Plain text Exclusive OR process with key.

4.2 Sub Byte

The AES Sub Bytes phase divides the input into bytes and passes them to a Substitution box. In contrast to DES, AES uses the same S-Box for all bytes. AES-S-Box implements inverse multiplication in Galois field (2^8) [12-13]. Table 2 shows the AES-S-Box. for example, in Table 2 shows the Sub Bytes, S-box (b0,04) = 8d

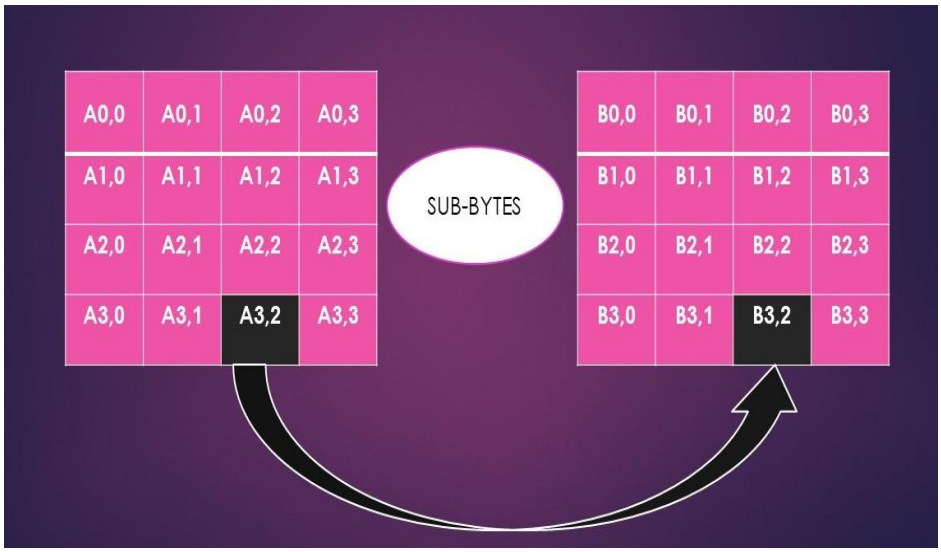

Figure 2. Sub Bytes process.

4.3 Shift Rows

The Shift Rows phase of AES shifts each row in the internal 128-bit state of the cipher. The rows in this phase refer to the standard representation of the AES internal state. 4x4 matrix with 1 byte in each cell. Internal status bytes are placed in a matrix of left-to-right rows and bottom columns. The Shift Rows operation shifts each of these rows to the left by a certain amount. Line numbers start at zero. The top row does not move at all; the next row moves one [14].

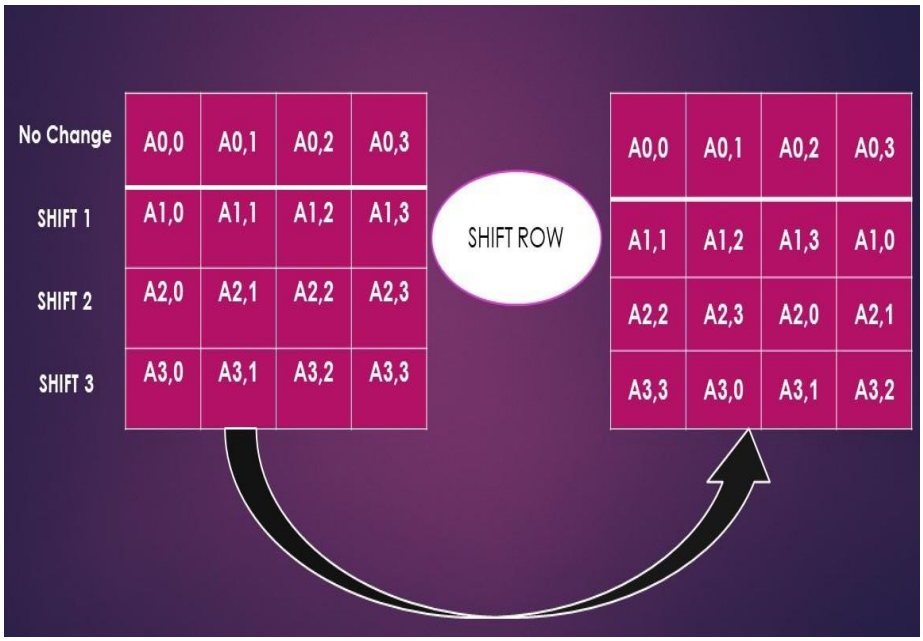

Figure 3. Shift Rows process.

4.4 Mix Columns

Like AES's Shift Rows phase, the Mix Columns phase provides diffusion by mixing the inputs around them. Unlike Shift Rows, Mix Columns performs matrix split operations by columns instead of rows. Mix Columns Shows a visual representation of the process. In contrast to standard matrix multiplication, Mix Columns performs matrix multiplication according to Galois field (2^8). Multiply the first column by the matrix to get the first column of the resulting matrix [15].

Figure 4. Mix Columns process.

4.5 Add Round Key

Very easy to understand features and conversions. The conversion function Add Round Key is a simple bitwise XOR operation. Exclusive OR for each 128-bit status matrix. 128-bit round keys for Exclusive OR and Figure 5. show the Gives output status matrix [16].

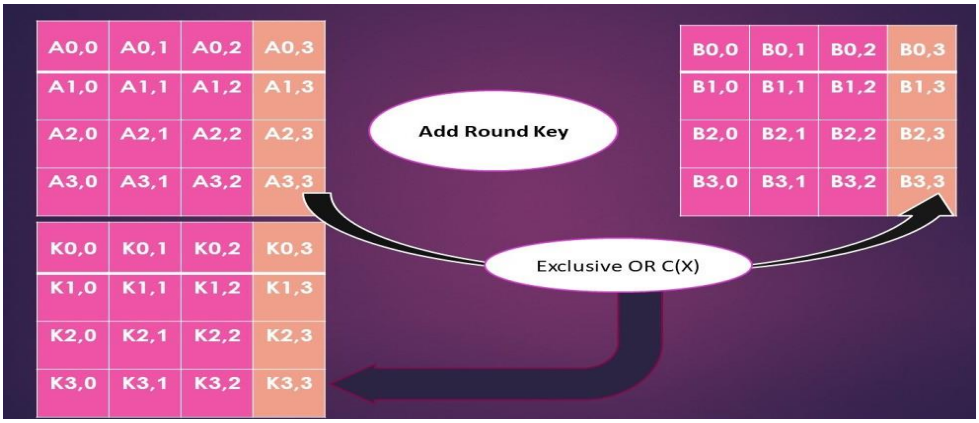

Figure 5. Round Key process.

5. Block Diagram of Advanced Encryption Standard (Encryption and Decryption).

Figure 6 shows the functional outline of the encryption and decryption process of the Advanced Encryption Standard and the decryption process of reverse operations (Sub Bytes, Shift Rows, Mix Columns, Add Round Key) [17].

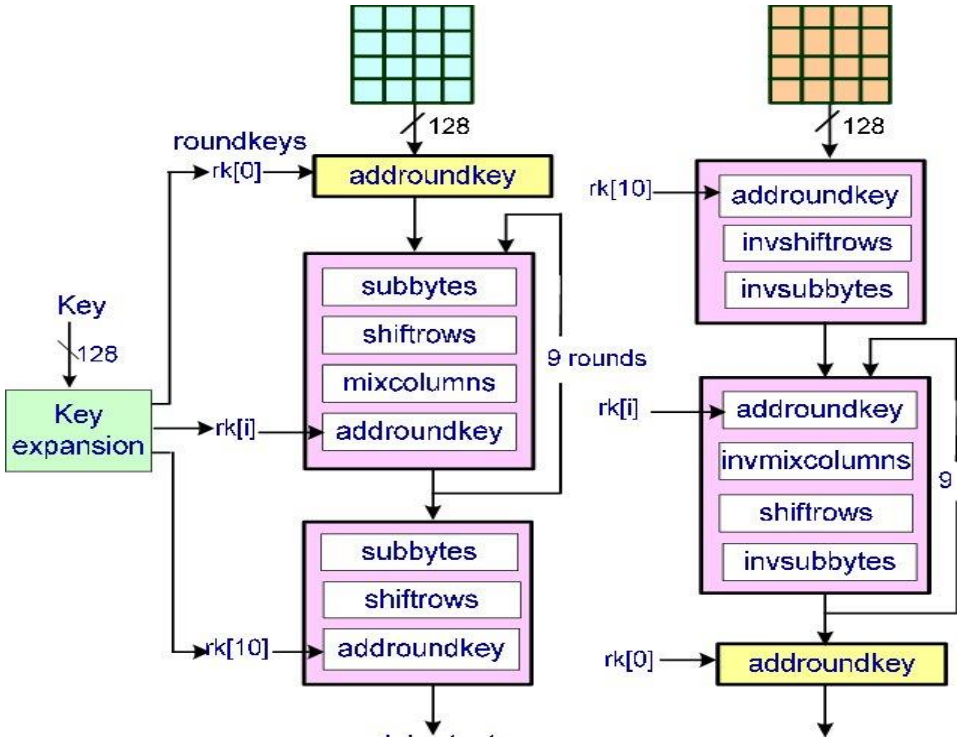

Figure 6. Encryption and Decryption.

6. Improve Substitution Box (New S-box)

The Substitution box is the most important part of cryptographic systems and determines its strength on a non-linear system. The new design will create two inverses of the Galois Field (2^8) to produce one inverse and replacement (1f, f1), (63, c4) and make the new Substitution box.

6.1 First Stage

The multiplicative inverse:

$$\text{inverse}=\begin{cases} (x)^{254} & x \neq 0 \\ 0 & x = 0 \end{cases} \tag{3}$$

The multiplicative inverse repeat:

$$\text{inverse s-box}(x)=(\text{s-box})^{-1}=\begin{cases} (x)^{254} & x \neq 0 \\ 0 & x = 0 \end{cases} \quad (4)$$

Equation (3) shows the inverse, Equation (4) shows the s-box inverse and Equation (5) show the new inverse

$$\text{New inverse s-box}=\text{inv}(x) \times \text{inverse s-box} \quad (5)$$

6.2 Second Stage

Equation (6) shows the New S-box. By replacement (1f, f1), (63, c4), [new matrix (G)] =F1, C=C4.

$$\text{New S-box}= [\text{new matrix (G)}] \times(x\text{-}1+B) \quad (6)$$

$$\text{New S-box}(x)=[\text{NEW MATRIX G}]\begin{bmatrix} 1,1,1,1,1,0,0,0 \\ 0,1,1,1,1,1,0,0 \\ 0,0,1,1,1,1,1,0 \\ 0,0,0,1,1,1,1,1 \\ 1,0,0,0,1,1,1,1 \\ 1,1,0,0,0,1,1,1 \\ 1,1,1,0,0,0,1,1 \\ 1,1,1,1,0,0,0,1 \end{bmatrix} \times (\text{s-box}(x)^{-1})+ \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

Table 3. The New S-box.

	00	**01**	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**0A**	**0B**	**0C**	**0D**	**0E**	**0F**
00	63	7c	f2	6b	ca	82	fa	59	09	83	1b	6e	53	d1	20	fc
10	af	a2	c0	72	2b	67	76	ab	39	be	cf	58	b3	d6	84	2f
20	50	3c	45	f9	10	ff	bc	b6	71	d8	34	a5	eb	27	07	12
30	f5	38	8f	40	85	33	fb	aa	9a	05	c3	23	cc	f7	26	93
40	62	ac	79	e4	ea	f4	08	ae	e9	87	df	28	0f	2d	16	bb
50	e7	c8	8d	d5	e0	32	49	06	8c	a1	bf	e6	e1	f8	69	d9
60	c6	b4	2e	25	0e	f6	66	b5	17	44	ec	13	88	90	dc	4f
70	86	c1	61	35	4b	bd	e8	dd	de	5e	46	ee	64	5d	c4	a7
80	b8	14	0b	db	7e	3d	19	73	57	b9	1d	9e	74	1f	8b	8a
90	0c	cd	97	5f	81	60	2a	22	78	ba	a6	1c	3e	70	03	48
A0	42	68	89	0d	8e	94	98	11	4e	a9	37	6d	24	5c	3a	0a
B0	55	ce	1e	9b	54	b0	99	41	95	91	d3	c2	7a	65	56	6c
C0	c7	04	96	18	fd	b7	3f	36	a3	51	9d	92	ef	d0	4d	43
D0	e5	f1	31	15	80	e2	b2	75	02	7f	9f	a8	da	21	f3	d2
E0	4c	4a	cb	6a	e3	29	3b	52	a4	9c	d4	ad	d7	fe	01	30
F0	5a	a0	2c	1a	b1	5b	00	ed	6f	c5	77	7b	47	f0	c9	7d

7. Analysis of S-box

The performance of block cyphers as strong as an alternate and surrogate AES depends on the structure of the S-box; the first layer of the AES system S-box must meet some essential characteristics to build a secure cryptosystem that can withstand. Below is a detailed performance analysis of the new s-box. Build S-box in MATLAB, a performance analysis of the S-box.

7.1 Balance

If the vector yield is equal to the number of 0s and 1s, the Boolean function should always be balanced. Boolean operations are offset if they meet the specified requirements. Where n is a Boolean variable, HW is the weight Hamming, and some are in the truth table. f (x). In the other world, f(x) {x | f(x) = 0} = {x | f (x) = 1}. For this case when n= 8 then (f (x)) = 128. Therefore, it accepts the balance standard for Strong s-box [18].

$$HWK(x)=\sum_{x=0}^{2n-1} F(x)=2^{n-1} \quad (7)$$

7.2 Bijective

Requires one-to-one mapping of input vectors to produce vectors. Bijective if each return makes a different value and is in the interval (0, 2n-1). The powerful s-box has various Table 2 throughput values in the gap (0,255). Along these lines, it accepts the objective standard of a Strong s-box [19].

7.3 Strict avalanche (SAC)

Strict avalanche (SAC) if a change of one bit in the input leads to at least 50% changes in the output bits, there is a strict collapse standard. A change of 50% is the ideal result for judging the S-box, and the process is done by taking the average value each time the difference. The analysis result is the Strong S-box shown in Table 4 [20]. The general study of the proposed Strong S-box and other AES S-box SACs is conducted in Table 5, and the proposed Strong SAC analysis is shown in Figure 7.

Table 4. New S-box (SAC).

Strict avalanche	Series 8	Series 7	Series 6	Series 5	Series 4	Series 3	Series 2	Series 1
1	124	116	124	116	124	140	120	116
2	132	136	132	124	120	128	132	140
4	116	124	116	136	124	124	124	128
8	124	120	120	140	116	124	124	124
16	136	120	120	124	120	120	120	124
32	140	128	116	124	128	128	140	120
64	124	132	128	120	112	128	136	128
128	124	124	140	112	140	124	116	128

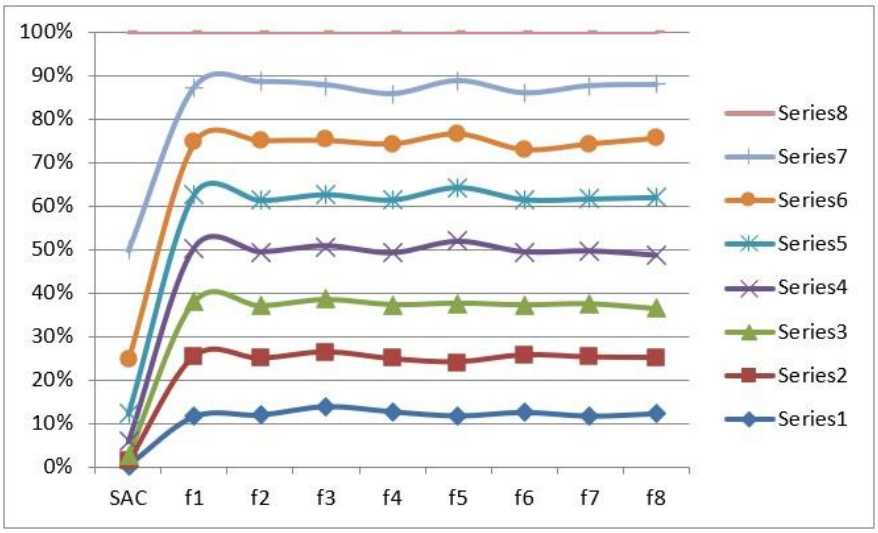

Figure 7. The SAC.

7.4 Bit Indepndence(BIC)

BIC requires that the yield bits are produced independently of each other. In other words, there shouldn't be any statistical pattern or dependencies between the yield bits of the yield vector. The elite or two bits of the S-box must be very non-linear. Thus, a distinctive feature of BIC is its nonlinear performance (BIC-nonlinearity) [21] shown in Table 5. So, the average nonlinear BIC is 112.

7.5 Periods between input and output (PD)

This test shows the distance of repetition of input and output elements. The new SBOX [1] has been implemented on the maximum possible distance between input and output, which makes the attack difficult, as shown in Table 5.

Table 4. Comparisons of S-box.

Performance index	*Optimal value*	*AES*	*GRAY Ref [22]*	*New S box*
Balance criteria	Yes	Yes	Yes	Yes
Bijective	Yes	Yes	Yes	Yes
SAC	0.5	0.504	0.508	0.494
Bit independence	112	112	112	112
Periods between input and output (PD)	increase	4	16	102

8. Implementation of Advanced Encryption Standard (New S-box)

In this section, the design and implementation of the advanced encryption standard is designed using the new substitution box by field-programmable gate array (FPGA), Vivado and zed board kit. The photograph of the FPGA shows in Figures 8, 9 and 10.

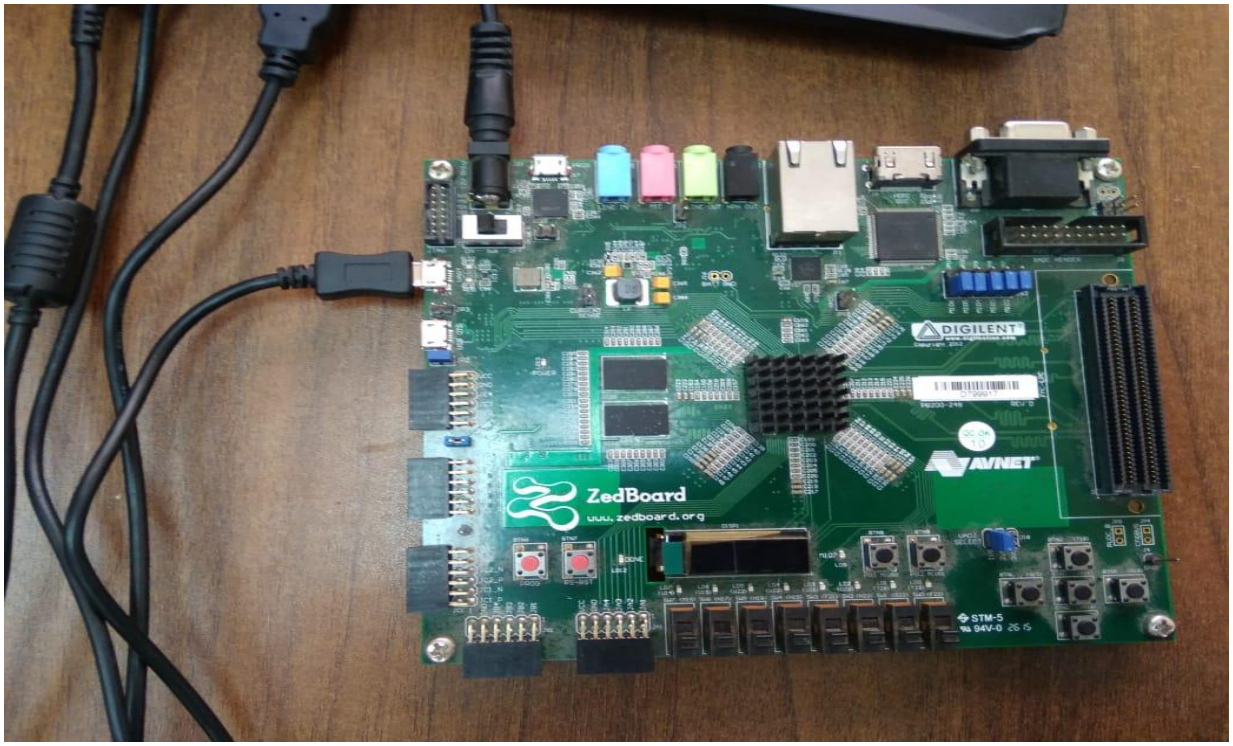

Figure 8. The ZedBoard kit (FPGA USING VHDL).

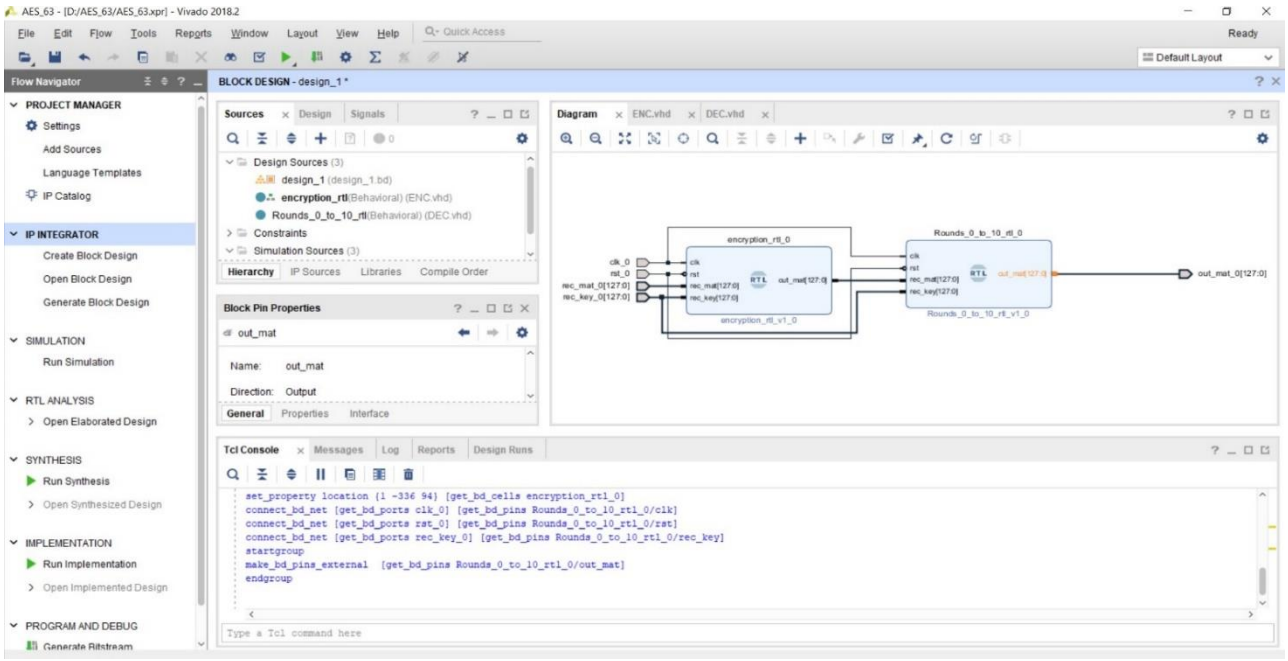

Figure 9. Design of advanced encryption standard BY VIVADO (FPGA).

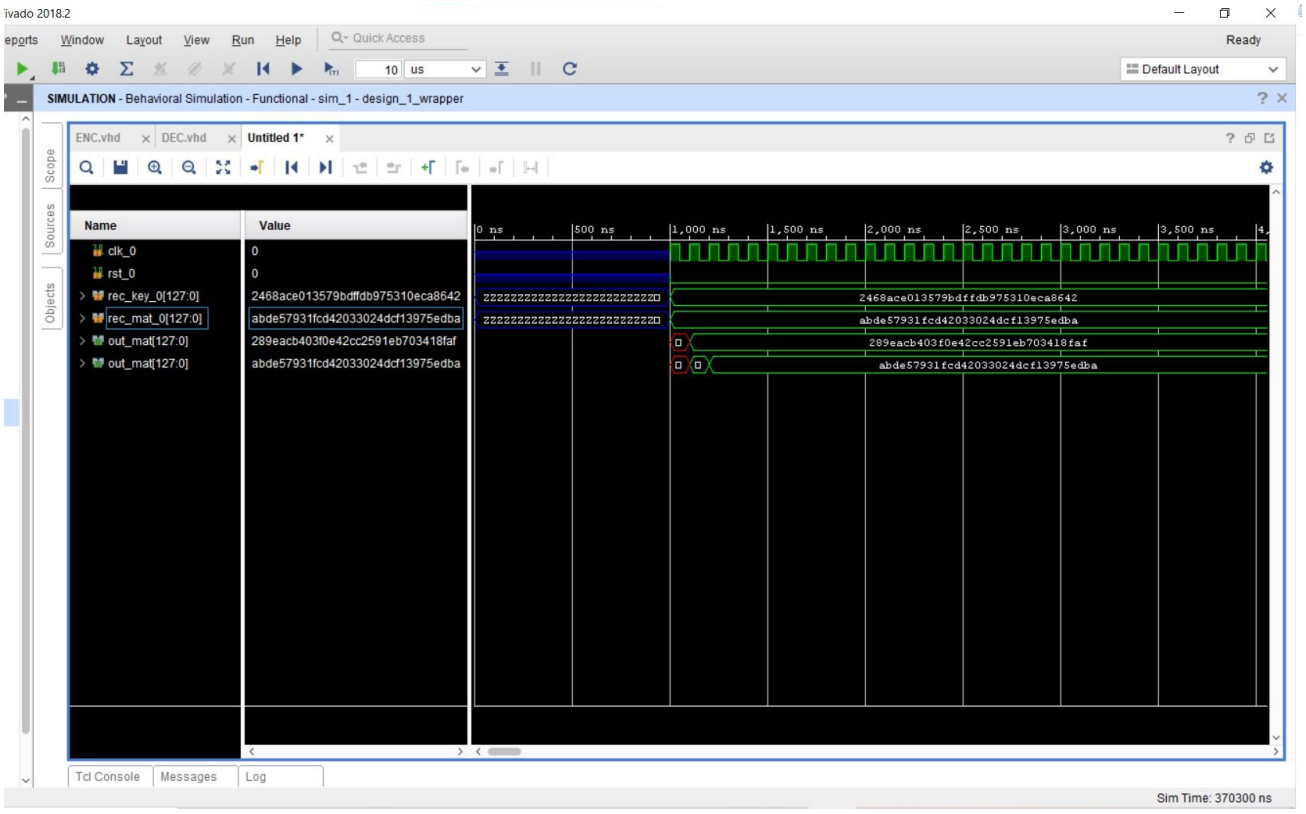

Figure 10. AES Simulation (Output FPGA Encryption and Decryption).

Table 5. Result (AES).

Plain text	abde57931fcd42033024dcf13975edba
Key	2468ace013579bdffdb975310eca8642
Encryption	289eacb403f0e42cc2591eb703418faf
Decryption	abde57931fcd42033024dcf13975edba

9. Conclusions

Covid-19's spread is thought to have resulted in the introduction of new strains of the disease. Because cryptography is critical in protecting our online banking transactions and electronic shopping from the actions of hackers, the development of cryptographic systems makes their results difficult to predict and increases the complexity for hackers to gain access to systems. The evolution of cryptographic systems makes it more difficult to predict their outcomes and makes it more difficult for hackers to gain access to systems.

References

1. El Sobky, W. I., Isamail, A. A., Mohra, A. S., & Hassan, A. M. (2021, July). Implementation Mini (Advanced Encryption Standard) by Substitution Box in Galois Field (2^4). In *2021 International Telecommunications Conference (ITC-Egypt)* (pp. 1-4). IEEE.
2. Stallings, W., Cryptography and Network Security - Principles and Practice, 7th Edition.; *Pearson Education India*,India,2017; P130-150.
3. Dawood, Omar. A., and Othman I. Hammadi. An analytical study for some drawbacks and weakness points of the AES cipher (rijndael algorithm). *QALAAI ZANIST SCIENTIFIC JOURNAL* 2.2 (2017):111-118.
4. Conti, V., & Vitabile, S. Design exploration of aes accelerators on fpgas and gpus. *Journal of Telecommunications and Information Technology* (2017).
5. Lapid, B., & Wool, A. (2018, August). Cache-attacks on the ARM TrustZone implementations of AES-256 and AES-256-GCM via GPU-based analysis. In *International Conference on Selected Areas in Cryptography* (pp. 235-256). Springer, Cham.
6. Andriani, R., Wijayanti, S. E., & Wibowo, F. W. (2018, November). Comparison of AES 128, 192 and 256 Bit Algorithm For Encryption And Description File. In *2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)* (pp. 120-124). IEEE.
7. Atteya, A. M., & Madian, A. H. (2014, June). A hybrid Chaos-AES encryption algorithm and its impelmention based on FPGA. In *2014 IEEE 12th International New Circuits and Systems Conference (NEWCAS)* (pp. 217-220). IEEE.
8. Chen, X. (2020, August). Implementing AES encryption on programmable switches via scrambled lookup tables. In *Proceedings of the Workshop on Secure Programmable Network Infrastructure* (pp. 8-14)..
9. El Sobky, Wageda I., et al. Enhancing Hierocrypt-3 Performance by Modifying Its S-Box and Modes of Operations. *J. Commun.* 15.12 (2020).
10. El Sobky, W. I, Saeed, H., Elwakeil,A. , Different Types of Attacks on Block Ciphers, *Int. J. Recent Technol. Eng*., vol. 9, no. 3, pp. 28–31, 2020.
11. Fernando, E., Agustin, D., Irsan, M., Murad, D. F., Rohayani, H., & Sujana, D. (2019, September). Performance Comparison of Symmetries Encryption Algorithm AES and DES With Raspberry Pi. In *2019 International Conference on Sustainable Information Engineering and Technology (SIET)* (pp. 353-357). IEEE.
12. Mei, Y. C., & Naziri, S. Z. M. (2011, December). The FPGA implementation of multiplicative inverse value of GF (2 8) generator using Extended Euclid Algorithm (EEA) method for Advanced Encryption Standard (AES) algorithm. In *2011 IEEE International Conference on Computer Applications and Industrial Electronics (ICCAIE)* (pp. 12-15). IEEE.
13. Srilaya, S., & Velampalli, S. (2018, May). Performance evaluation for des and AES algorithms-an comprehensive overview. In *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)* (pp. 1264-1270). IEEE.
14. Hosseinkhani, R., & Javadi, H. H. S Using cipher key to generate dynamic S-box in AES cipher system." *International Journal of Computer Science and Security (IJCSS)* 6.1 (2012): 19-28.
15. Satoh, A., Morioka, S., Takano, K., & Munetoh, S. (2001, December). A compact Rijndael hardware architecture with S-box optimization. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 239-254). Springer, Berlin, Heidelberg.
16. Lo, Owen, William J. Buchanan, and Douglas Carson. Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA). *Journal of Cyber Security Technology* 1.2 (2017): 88-107.
17. Daemen, Joan, and Vincent Rijmen. Specification of Rijndael. *The Design of Rijndael*. Springer, Berlin, Heidelberg, 2020. 31-51.
18. Pei, Chao, et al. Trade-off of security and performance of lightweight block ciphers in Industrial Wireless Sensor Networks. *EURASIP Journal on Wireless Communications and Networking* 2018.1 (2018): 1-18..
19. Özkaynak, Fatih. An analysis and generation toolbox for chaotic substitution boxes: A case study based on chaotic labyrinth rene thomas system. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering* 44.1 (2020): 89-98.
20. Sanap, S. D., & More, V. (2021, May). Performance Analysis of Encryption Techniques Based on Avalanche effect and Strict Avalanche Criterion. In *2021 3rd International Conference on Signal Processing and Communication (ICPSC)* (pp. 676-679). IEEE.
21. Liu, Liyan, Yingqian Zhang, and Xingyuan Wang. "A novel method for constructing the S-box based on spatiotemporal chaotic dynamics." *applied sciences* 8.12 (2018): 2650.
22. Tran, M. T., Bui, D. K., & Duong, A. D. (2008, December). Gray S-box for advanced encryption standard. In *2008 international conference on computational intelligence and security* (Vol. 1, pp. 253-258). IEEE.