1

by Alam Syah

Submission date: 11-Jun-2021 09:39AM (UTC+0700)
Submission ID: 1604426693
File name: 08073857.pdf (258.81K)
Word count: 3302
Character count: 15286

AES S-Box Construction Using Different Irreducible Polynomial and Constant 8-bit Vector

Alamsyah[1,2], Agus Bejo[1], Teguh Bharata Adji[1]
[1]Department of Electrical Engineering and Information Technology, Universitas Gadjah Mada, Indonesia
[2]Department of Computer Science, Universitas Negeri Semarang, Indonesia
alamsyah.16@mail.ugm.ac.id, alamsyah@mail.unnes.ac.id, agusbj@ugm.ac.id, adji@ugm.ac.id

***Abstract*— S-box plays a major role in the AES algorithm. The strength of S-box depends on the design and algebraic constructions. In this paper, the construction of S-box will be built using a basic polynomial equation and the addition of a constant 8-bit vector different from the standard AES. The quality of the created S-box is evaluated by measuring several standard criteria such as nonlinearity, strict avalanche criterion (SAC), and bit independence criterion-nonlinearity (BIC-Nonlinearity). The evaluation shows that the values of nonlinearity, SAC, and BIC-Nonlinearity are 112, 0.4995, and 112 respectively. This research also found that the proposed S-box construction method outperforms other existing S-boxes construction methods.**

Keywords—Advanced Encryption Standard (AES), Substitution Box (S-box), Irreducible Polynomial, Nonlinearity, Strict Avalanche Criterion (SAC), Bit Independent Criterion (BIC).

I. Introduction

S-box is the key component of Data Encryption Standards (DES), International Data Encryption Algorithm (IDEA), and Advanced Encryption Standard (AES). S-box is used to randomize input bits that will result in output bits.

An $m \times n$ S-box is a nonlinear transformation of m input bits into n output bits, represented as S: $\{0,1\}^m \rightarrow \{0,1\}^n$. This S-box can be considered as a combination of n Boolean functions. If $m = n$, then the number of input bits are the same as the number of output bits. For example, an 8×8 S-box has eight Boolean functions composed of 8 input bits and 8 output bits [1].

There are many ways in designing an 8x8 S-box, some of them are with the use of algebraic techniques, heuristic methods, power mapping technologies, analytical approach, and cellular automata [2]. For example, Wadi and Zaenal [3] built new S-box using a simple method by merely concatenating two groups of hexadecimal numbers. The main motivation in building this simple S-box is to accelerate the process of encryption and decryption. Consequently, this simple S-box decreases hardware requirement and computation cost. Table 1 shows the simple S-box. However, Yap et al. [4] criticized that the S-box in [3] is unsafe i.e. suffers from differential attacks. However, the research did not suggest any better S-box construction.

TABLE I. S-BOX PROPOSED BY WADI AND ZAINAL [3]

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48
79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64
95	94	93	92	91	90	89	88	87	86	85	84	83	82	81	80
111	110	109	108	107	106	105	104	103	102	101	100	99	98	97	96
127	126	125	124	123	122	121	120	119	118	117	116	115	114	113	112
143	142	141	140	139	138	137	136	135	134	133	132	131	130	129	128
159	158	157	156	155	154	153	152	151	150	149	148	147	146	145	144
250	234	218	202	186	170	169	168	167	166	165	164	163	162	161	160
251	235	219	203	187	171	185	184	183	182	181	180	179	178	177	176
252	236	220	204	188	172	201	200	199	198	197	196	195	194	193	192
253	237	221	205	189	173	217	216	215	214	213	212	211	210	209	208
254	238	222	206	190	174	233	232	231	230	229	228	227	226	225	224
255	239	223	207	191	175	249	248	247	246	245	244	243	242	241	240

Hence, this paper aims to propose a stronger S-box construction compared to previous works. In this proposed S-box, irreducible polynomial equation $m(x) = x^8 + x^6 + x^5 + x + 1$ with an additional constant 8-bit vector is used. The polynomial is chosen since it is stated in [5][6] to be the most optimal solution for S-box construction.

II. Related Works

Previous researchers developed several S-box constructions which will be discussed in the following lines.

Zaïbi et al. [7] developed an active S-box based on one-dimensional chaotic map i.e. logistic and piecewise linear chaotic map (PWLCM). This research results in very low linear and differential probabilities. Moreover, Zaïbi et al. [8] developed a dynamic S-box using the combination of two chaotic maps i.e. one-dimensional and three-dimensional piecewise linear maps. The dynamic S-box was tested using The NIST (National Institute of Standards and Technology) test package and the result was that the dynamic S-box had the lowest linear approximation probability.

978-1-5090-5569-2/17/$31.00 ©2017 IEEE

Ahmad et al. [9] constructed an S-box based on Chaos Method. This method produced an efficient way to build a strong S-box. Ahmad et al. [10] also constructed another S-box using the classical method of Fisher-Yates shuffle technique. The result was the construction of S-box which is consistent and secured. Moreover, Ahmad et al. [11] developed an approach based on high-dimensional chaotic system namely the Chen, the Rossler, and the Chua. The result was the construction of S-box that is efficient and secured.

Das et al. [12] developed a new S-box, which was dynamically constructed using automatically generated irreducible polynomials. Each generated polynomial will generate different encryption – decryption performance. Consequently, the security will also increase. Wang and Sun [5] conducted a research on the possibility of irreducible polynomial $m(x) = x^8 + x^6 + x^5 + x + 1$, which was used in building an S-box. This irreducible polynomial was found to be optimal. Meanwhile, a research by Gangadaril and Ahamed [6] also produced irreducible polynomial $m(x) = x^8 + x^6 + x^5 + x + 1$ that is better than AES' irreducible polynomial.

Another research by Isa et al. [13] made a strong S-box based on heuristic method. The algorithm is inspired by bee waggle dance. The generated S-box has high nonlinearity, low differential uniformity, and high algebraic degree. Guesmi et al. [14] developed an active S-box based on chaos function and genetic algorithm technique which has high immunity against differential cryptanalysis. Meanwhile, Noughabi and Sadeghiyan [15] utilized a neural system to construct S-box. The outcome demonstrated that the learning of the neural system plays important role in the cryptography and cryptanalysis fields.

In this paper, a novel approach is proposed using irreducible polynomial $m(x) = x^8 + x^6 + x^5 + x + 1$ that was presented in [5] and [6]. This irreducible polynomial is used for the multiplicative inverse in Galois Field 2^8 ($GF(2^8)$). Finally, the novel S-box will be created utilizing Affine Mapping AES and an additional constant 8-bit vector (00000001) [16]. For each input element A_i in $GF(2^8)$, $B_i' = A^{-1}$ and B_i output are generated from the input element A_i. The S-box can be seen as a two-stage mathematical transformation as illustrated in Fig.1.

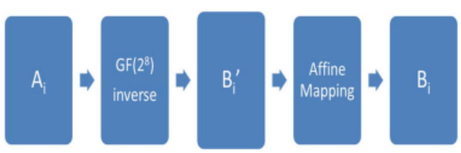

Figure 1. The two operations within the proposed S-box

III. Proposed Method

This section introduces our technique for constructing a cryptographically strong 8×8 S-box using irreducible polynomial $m(x) = x^8 + x^6 + x^5 + x + 1$ and AES Afinne Mapping.

Table II shows a multiplicative inverse table using irreducible polynomial $m(x) = x^8 + x^6 + x^5 + x + 1$ in $GF(2^8)$. The result of the multiplicative inverse will be inserted into a bitwise vector $B' = (b'_7, \ldots, b'_0)$ of the Affine Mapping given by Eq.(1). The result of the Eq.(1) will be the construction of S-box as shown in Table III.

The testing of the developed S-box in this paper includes balance, bijective, nonlinearity, strict avalanche criterion (SAC), and bit independence criterion (BIC) which will be explained as follows.

TABLE II. Proposed Multiplicative Inverse

0	1	177	222	233	74	111	140	197	165	37	193	134	84	70	231
211	93	227	133	163	52	209	237	67	166	42	99	35	158	194	119
216	45	159	28	192	10	243	171	224	181	26	98	217	33	199	189
144	86	83	234	21	162	128	121	160	91	79	229	97	73	138	205
108	154	167	24	254	124	14	230	96	61	5	232	200	130	228	58
112	106	235	50	13	135	49	145	221	246	161	57	210	17	239	191
72	60	43	27	152	213	117	151	187	184	81	113	64	155	141	6
80	107	156	142	150	102	195	31	129	55	149	178	69	255	215	136
54	120	77	201	226	19	12	85	127	214	62	204	7	110	115	157
48	87	175	248	179	122	116	103	100	212	65	109	114	143	29	34
56	90	53	20	196	9	25	66	183	172	242	39	169	182	249	146
223	2	123	148	225	41	173	168	105	186	185	104	198	47	238	95
36	11	30	118	164	8	188	46	76	131	219	253	139	63	250	245
236	22	92	16	153	101	137	126	32	44	252	202	247	88	3	176
40	180	132	18	78	59	71	15	75	4	51	82	208	23	190	94
241	240	170	38	251	207	89	220	147	174	206	244	218	203	68	125

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \bmod 2 \quad (1)$$

TABLE III. Proposed S-Box

1	30	131	2	77	0	128	10	42	14	129	86	204	75	132	247
153	172	139	237	76	111	167	49	231	47	36	4	195	197	119	137
64	121	218	116	73	199	122	180	170	255	54	27	95	253	20	7
127	117	22	108	147	83	142	51	109	238	99	201	58	33	72	210
161	185	48	8	225	80	187	232	37	136	98	82	177	176	214	213
212	227	115	45	154	211	12	96	35	25	114	244	134	239	15	57
62	151	59	41	135	219	183	34	69	100	40	203	198	166	21	67
55	252	251	52	61	103	104	85	145	78	28	162	165	254	229	118
81	44	93	174	148	209	133	84	113	250	169	205	92	159	245	228
19	106	200	163	189	18	168	120	89	196	217	190	234	43	107	220
235	241	112	140	53	230	23	248	193	233	101	191	138	222	188	65
29	63	13	3	181	5	246	149	194	90	123	221	11	71	16	146
158	216	74	150	17	249	24	88	66	175	97	192	87	182	157	56
46	178	179	240	152	70	105	110	226	102	223	143	6	207	32	156
26	224	242	206	124	202	155	164	31	125	50	9	184	173	38	141
68	91	171	160	130	236	208	60	94	215	243	39	126	144	186	79

3.1 Balance

A Boolean function is said to be balanced if it meets a condition formulated in Eq.(2):

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

where n is a Boolean variable and H_W is Hamming weight, which is the number of ones in the truth table of $f(x)$. In other words, $f(x)$, $\#\{x \mid f(x) = 0\} = \#\{x \mid f(x) = 1\}$. In this case, since n = 8 then $H_W(f(x)) = 128$. Therefore, it accepts the balance criterion [1].

3.2. Bijective

An $n \times n$ S-box is bijective if each output produces a different value and is in the interval $[0, 2^n\text{-}1]$. The proposed S-box has different output values in the interval [0, 255]. Therefore, it accepts the bijective criterion [17].

3.3 Nonlinearity

A Boolean function is said to be nonlinearity if it meets Eq.(3):

$$NL(f(x)) = \min d(f(x), g(x)) \quad (3)$$

$d(f(x),g(x))$ is the Hamming distance to the set of all n-variable of Affine functions. For two Boolean functions, the Hamming distance $d(f(x),g(x))$ is defined as $H_W(f(x)+g(x))$ [1] [18].

The proposed S-box has nonlinearity of 112 for all Boolean functions, as shown in Table IV. Therefore, the average nonlinearity is 112.

TABLE IV. NONLINEARITY OF PROPOSED S-BOX

112	112	112	112	112	112	112	112

3.4. Strict avalanche criterion (SAC)

SAC is defined as if input bit i changes, then each bit element of the output matrix will change with a probability of 0.5 [18]. This SAC is defined as Eq.(4):

$$\delta(x) = \left(\frac{1}{2^n}\sum_{i=1}^{n} f(x) \oplus f(x \oplus c_i^n)\right) \quad (4)$$

c_i^n implies an n dimensional vector with Hamming weight 1 at the i^{th} position. If all elements in the output matrix have values close to 0.5, then the cryptographical function satisfies the strict avalanche criterion.

The proposed S-box has the average SAC of 0.4995 and the SAC matrix is shown in Table V.

TABLE V. STRICT AVALANCHE CRITERION OF PROPOSED S-BOX

0.5	0.4688	0.4844	0.4844	0.5156	0.4844	0.5313	0.5156
0.5156	0.5	0.4688	0.4844	0.5313	0.4688	0.4844	0.5156
0.5156	0.5156	0.5	0.4688	0.5469	0.5156	0.4688	0.4844
0.4844	0.5156	0.5156	0.5	0.4844	0.4844	0.5156	0.4844
0.4844	0.4844	0.5156	0.5156	0.5156	0.5156	0.4844	0.5156
0.5156	0.4844	0.4844	0.5156	0.5156	0.4531	0.5156	0.5156
0.5156	0.5156	0.4844	0.4844	0.5313	0.5313	0.4531	0.4531
0.4531	0.5156	0.5156	0.4844	0.5313	0.4688	0.5313	0.5156

3.5. Bit independence criterion (BIC)

The bit independence is determined by testing an individual bit at the input of the cipher by performing toggle operation [19]. The exclusive or of two output bits in an S-box, $f_i \oplus f_j$, should be highly nonlinear. Thus, the important aspect of the BIC is its nonlinear (BIC-nonlinearity) behavior which is shown in Table VI. Therefore, the average BIC nonlinearity is 112.

TABLE VI. BIC-NONLINEARITY

-	112	112	112	112	112	112	112
112	-	112	112	112	112	112	112
112	112	-	112	112	112	112	112
112	112	112	-	112	112	112	112
112	112	112	112	-	112	112	112
112	112	112	112	112	-	112	112
112	112	112	112	112	112	-	112
112	112	112	112	112	112	112	-

IV. RESULT AND DISCUSSION

The performance of the proposed method is measured by the proposed S-box balance, bijective, nonlinearity, strict avalanche criterion (SAC), and bit independence criterion (BIC). Performance comparison of nonlinearity, SAC, and BIC is shown in Table VII. The table demonstrates the strength of the proposed S-box compared with available S-boxes using various methods. AES S-box and the proposed S-box have the highest average scores of 112 for nonlinearity and BIC-nonlinearity. Whilst SAC of the proposed S-box is 0.4995 that outperforms other methods.

TABLE VII. PERFORMANCE COMPARISON

S-Box	Avg. Nonlinearity	Avg. SAC	BIC-Nonlinearity
Proposed	112	0.4995	112
AES	112	0.5049	112
In[2]	105	0.4907	-
In[10]	106	0.4965	-
In[11]	106	0.5048	-
In[13]	108	-	-
In[14]	108	0.4971	104

V. CONCLUSION

The proposed method generates 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 the novel S-box is tested using balance, bijective, nonlinearity, SAC, and BIC (BIC-nonlinearity). The results of the testing show that the proposed S-box is a balanced and is bijective. The testing also gives 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 has better security level compared to other existing S-boxes.

For future research, the construction of more powerful S-box by increasing its criteria is suggested so that the S-box becomes resistant to linear and differential cryptanalysis.

REFERENCES

[1] I. Hussain and T. Shah, "Literature survey on nonlinear components and chaotic nonlinear components of block ciphers," *Nonlinear Dyn.*, vol. 74, no. 4, pp. 869–904, 2013.

[2] M. Ahmad and H. Haleem, "A New Chaotic Substitution Box Design for Block Ciphers," in *International Conference on Signal Processing and Integrated Networks (SPIN)*, 2014, no. 1, pp. 255–258.

[3] S. M. Wadi and N. Zainal, "High Definition Image Encryption Algorithm Based on AES Modification," *Wirel. Pers. Commun.*, vol. 79, no. 2, pp. 811–829, 2014.

[4] W. Yap, R. C, W. Phan, and B.-M. Goi, "Cryptanalysis of a High-Definition Image Encryption Based on AES Modification," *Wirel. Pers. Commun.*, vol. 88, no. 3, pp. 685–699, 2016.

[5] D. Wang and S.-L. SUN, "Replacement and Structure of S-boxes in Rijndael," in *International Conference on Computer Science and Software Engineering*, 2008, pp. 782–784.

[6] B. R. Gangadaril and S. R. Ahamed, "Analysis and Algebraic Construction of S-Box for AES algorithm using Irreducible Polynomials," in *Eighth International Conference on Contemporary Computing (IC3)*, 2015.

[7] G. Zaibi, A. Kachouri, F. Peyrard, and Daniele Fournier-Prunaret, "On Dynamic chaotic S-BOX," in *Global Information Infrastructure Symposium*, 2009, no. 2, pp. 1–5.

[8] G. Zaïbi, F. Peyrard, A. Kachouri, and M. Samet, "A new design of dynamic S - Box based on two chaotic maps .," in *ACS/IEEE International Conference on Computer Systems and Applications - AICCSA 2010*, 2011.

[9] M. Ahmad, H. Chugh, A. Goel, and P. Singla, "A Chaos Based Method for Efficient Cryptographic S-box Design," in *Security in Computing and Communications, International Symposium*, 2013, pp. 130–137.

[10] M. Ahmad, P. M. Khan, and M. Z. Ansari, "A Simple and Efficient Key-Dependent S-Box Design Using Fisher-Yates Shuffle Technique," in *Recent Trends in Computer Networks and Distributed Systems Security, Second International Conference*, 2014, pp. 540–550.

[11] M. Ahmad and S. Alam, "A Novel Approach for Efficient S-Box Design Using Multiple High-Dimensional Chaos," in *Fourth International Conference on Advanced Computing & Communication Technologies*, 2014, pp. 95–99.

[12] I. Das, S. Roy, S. Nath, and S. Mondal, "Random S-Box Generation in AES by changing Irreducible polynomial," in *International Conference on Communications, Devices and Intelligent Systems (CODIS)*, 2012, no. 2, pp. 556–559.

[13] H. Isa, N. Jamil, and M. R. Z. Aba, "Construction of Cryptographically Strong S-Boxes Inspired by Bee Waggle Dance," *New Gener. Comput.*, vol. 7, pp. 221–238, 2016.

[14] R. Guesmi, M. A. Ben Farah, A. Kachouri, and M. Samet, "A novel design of Chaos based S-Boxes using genetic algorithm techniques," *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. AICCSA*, vol. 2014, pp. 678–684, 2014.

[15] M. N. A. Noughabi and B. Sadeghiyan, "Design of S-boxes based on neural networks," *ICEIE 2010 - 2010 Int. Conf. Electron. Inf. Eng. Proc.*, vol. 2, no. Iceie, pp. 172–178, 2010.

[16] C. Paar and J. Pelzl; *Understanding Cryptography*, 1st ed., vol. 1. Springer-Verlag Berlin Heidelberg, 2010.

[17] D. Lambić, "A novel method of S-box design based on chaotic map and composition method," *Chaos, Solitons, and Fractals*, vol. 58, pp. 16–21, 2014.

[18] R. Guesmi, M. Amine, B. Farah, A. Kachouri, and M. Samet, "Chaos-based Designing of a Highly Nonlinear S-box using Boolean Functions," in *12th International Multi-Conference on Systems, Signals & Devices*, 2015, pp. 1–5.

[19] M. Asif and G. Abdul, "A Scheme for Obtaining Secure S-Boxes Based on Chaotic Baker ' s Map," *3D Res.*, vol. 5, pp. 1–8, 2014.

1

ORIGINALITY REPORT

14%	7%	13%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Iqtadar Hussain, Tariq Shah, Muhammad Asif Gondal, Hasan Mahmood. "S8 affine-power-affine S-boxes and their applications", Neural Computing and Applications, 2012 Publication	2%
2	"PWLCM-Based Random Search for Strong Substitution-Box Design", Advances in Intelligent Systems and Computing, 2016. Publication	1%
3	Bimal Roy. "Cyptographic Algorithms", Handbook of Applied Algorithms, 02/02/2008 Publication	1%
4	Ghada Zaibi, Fabrice Peyrard, Abdennaceur Kachouri, Daniele Fournier-Prunaret, Mounir Samet. "A new design of dynamic S-Box based on two chaotic maps", ACS/IEEE International Conference on Computer Systems and Applications - AICCSA 2010, 2010 Publication	1%
5	dspace.lboro.ac.uk Internet Source	1%

6	quspace.qu.edu.qa Internet Source	1 %
7	arro.anglia.ac.uk Internet Source	1 %
8	Athmane Seghier, Jianxin Li. "Chapter 24 Parallel Steepest Ascent Hill-Climbing for High Nonlinear Boolean and Vectorial Boolean Functions (S-Boxes)", Springer Science and Business Media LLC, 2020 Publication	1 %
9	Bahram Rashidi. " Lightweight 8 ‐ bit S ‐ box and combined S ‐ box/S ‐ box for cryptographic applications ", International Journal of Circuit Theory and Applications, 2021 Publication	1 %
10	Ricardo Soto, Broderick Crawford, Francisco Gonzalez, Rodrigo Olivares. "Human behaviour based optimization supported with self-organizing maps for solving the S-box design Problem", IEEE Access, 2021 Publication	1 %
11	researchr.org Internet Source	1 %
12	Ghada Zaibi. "On dynamic chaotic S-BOX", 2009 Global Information Infrastructure Symposium, 06/2009	<1 %

Publication

13	sciencepubco.com Internet Source	<1 %
14	Herman Isa, Norziana Jamil, Muhammad Reza Z'aba. "Construction of Cryptographically Strong S-Boxes Inspired by Bee Waggle Dance", New Generation Computing, 2016 Publication	<1 %
15	Imran Shahzad, Qaiser Mushtaq, Abdul Razaq. "Construction of New S-Box Using Action of Quotient of the Modular Group for Multimedia Security", Security and Communication Networks, 2019 Publication	<1 %
16	Kwangjo Kim. "Chapter 5 Construction of DES-like S-boxes based on Boolean functions satisfying the SAC", Springer Science and Business Media LLC, 1993 Publication	<1 %
17	Ruming Yin, Jian Yuan, Jian Wang, Xiuming Shan, Xiqin Wang. "Designing key-dependent chaotic S-box with larger key space", Chaos, Solitons & Fractals, 2009 Publication	<1 %
18	academic.odysci.com Internet Source	<1 %

19	Communications in Computer and Information Science, 2015. Publication	<1 %
20	Zaid Bin Faheem, Asim Ali, Muhamad Asif Khan, Muhammad Ehatisham Ul ‐ Haq, Waqar Ahmad. "Highly dispersive substitution box (S ‐ box) design using chaos", ETRI Journal, 2020 Publication	<1 %
21	Musheer Ahmad, Eesa Al-Solami, Ahmed Mohammed Alghamdi, Muhammad Awais Yousaf. "Bijective S-Boxes Method Using Improved Chaotic Map-Based Heuristic Search and Algebraic Group Structures", IEEE Access, 2020 Publication	<1 %
22	Saleh Ibrahim, Hesham Alhumyani, Mehedi Masud, Sultan S. Alshamrani et al. "Framework for Efficient Medical Image Encryption Using Dynamic S-Boxes and Chaotic Maps", IEEE Access, 2020 Publication	<1 %
23	dokumen.pub Internet Source	<1 %

Exclude quotes On

Exclude matches < 10 words

Exclude bibliography On

1

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4