paper

by wer say

S-box Construction of Highly Strict Avalanche Criterion Using Algebraic Technique

Alamsyah
Department of Electrical Engineering and Information Technology, Universitas Gadjah Mada
Department of Computer Science, Universitas Negeri Semarang
Indonesia
alamsyah.16@mail.ugm.ac.id, alamsyah@mail.unnes.ac.id

Agus Bejo
Department of Electrical Engineering and Information Technology, Universitas Gadjah Mada
Indonesia
agusbj@ugm.ac.id

Teguh Bharata Adji
Department of Electrical Engineering and Information Technology, Universitas Gadjah Mada
Indonesia
adji@ugm.ac.id

***Abstract*—A strong S-box construction will determine the level of data security during the data encryption and decryption process. One of the methods for S-boxes construction is using algebraic technique. In algebraic technique, S-box construction is built based on the selected irreducible polynomial. In this paper, the construction of S-boxes will be discussed. The constructed S-boxes are S-box$_1$, S-box$_2$, and S-box$_3$ that use three irreducible polynomials i.e. $p_1(x) = x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$, $p_2(x) = x^8 + x^6 + x^3 + x^2 + 1$, and $p_3(x) = x^8 + x^4 + x^3 + x^2 + 1$ respectively. The resulting S-boxes will be tested using strict avalanche criterion, showing that S-box$_3$ is the best S-box with a value of 0.49658 compared to S-box$_1$, S-box$_2$, and S-boxes from previous researchers.**

***Keywords*—AES, S-box, irreducible polynomial, algebraic technique, strict avalanche criterion.**

I. INTRODUCTION

S-box is a substitution box that functions to randomize bits in the process of encryption and decryption [1] . The strength of S-box depends on the method of building S-box construction. One of the most popular methods of constructing S-boxes is the algebraic technique [2].

In the algebraic technique, the main component in building S-box is the irreducible polynomial [3]. An irreducible polynomial is a polynomial that has a factor of 1 and itself [4]. The precise irreducible polynomial selection will produce a strong S-box [5].

One of the methods to measure the strength of S-box is to calculate the strict avalanche criterion (SAC) value [1]. With SAC, if there is a change of 1 bit input, then the change in bit output can be calculated. The ideal value of the SAC is 0.5. That is, if there is 1 bit input changes, then half of the output bits change. The closer the SAC value to 0.5, the stronger the S-box is generated [6].

S-box construction was done by previous studies with various methods [7][8][9][10][11][12]. Unfortunately, the methods resulted in SAC values that are still far from the ideal value of 0.5.

Hence, this paper aims to propose S-boxes construction using algebraic technique that uses irreducible polynomials $p_1(x) = x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$, $p_2(x) = x^8 + x^6 + x^3 + x^2 + 1$, and $p_3(x) = x^8 + x^4 + x^3 + x^2 + 1$ [13][14][15]. The resulting S-boxes will be tested using SAC. The selected S-box is the best S-box that have the highest SAC value compared to previous studies.

II. RELATED WORKS

In this section, we will discuss S-boxes construction with various methods from previous researchers.

Girija and Singh [7] developed S-box built on functions that generate random numbers at interval [0..255]. The S-box was then fixed with a double random phase encoding (DRPE) system. The result was a random S-box as shown in Table I.

TABLE I. S-BOX PROPOSED BY GIRIJA AND SINGH [7]

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

Farwa et al. [8] built an S-box with an algebraic technique without using irreducible polynomial and affine mapping. Instead, the research uses a specific nonlinear and iterative map defined in GF (2^8). Table II shows the S-box made by Farwa et al.

TABLE II. S-BOX PROPOSED BY FARWA ET AL.[8]

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

Çavuşoğlu et al. [9] developed an S-box design by placing an 8-bit value taken from a random number generator (RNG) to be placed into a value in the S-box table. The 8-bit value was converted into decimal value. If the resulting decimal value was available in the S-box table, the decimal value was not used. The decimal value would be added to the S-box table if the decimal value was not yet available in the S-box table. Thus, the decimal value in the 0-255 interval will be uniquely placed in the S-box table as shown in Table III.

TABLE III. S-BOX PROPOSED BY ÇAVUŞOĞLU ET AL.[9]

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

Another research by Wadi and Zaenal [10] built new S-box using a simple method by combining two hexadecimal numbers and sorting them. Proposed S-boxes based on a chaotic system by Khan et al. [11] and Çavusoglu et al. [12].

In this paper, a new approach is presented in building S-boxes. The S-boxes are presented based on the irreducible polynomials, $p_1(x) = x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$, $p_2(x) = x^8 + x^6 + x^3 + x^2 + 1$, and $p_3(x) = x^8 + x^4 + x^3 + x^2 + 1$ [13][14][15]. Based on the irreducible polynomials, multiplicative inverse tables are built. Each element in the inverse multiplicative table is applied to an affine transformation so that a robust S-box is generated.

III. PROPOSED METHOD

In this section we will introduce a strong S-box construction using algebraic technique. The S-boxes are built based on irreducible polynomial $p_1(x) = x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$, $p_2(x) = x^8 + x^6 + x^3 + x^2 + 1$, and $p_3(x) = x^8 + x^4 + x^3 + x^2 + 1$ [13][14][15]. Based on irreducible polynomials $p_1(x)$, $p_2(x)$, and $p_3(x)$ generated inverse multiplicative tables as shown in Table IV, Table V, and Table VI.

Each element contained in the inverse multiplicative table shown in Tables IV, V, and VI is applied to an affine transformation defined in Equation 1 [3]. The result are S-box$_1$ built by irreducible polynomial $p_1(x) = x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$ and multiplicative inverse p_1, S-box$_2$ built by irreducible polynomial $p_2(x) = x^8 + x^6 + x^3 + x^2 + 1$ and multiplicative inverse p_2, and S-box$_3$ built by irreducible polynomial $p_3(x) = x^8 + x^4 + x^3 + x^2 + 1$ and multiplicative invers p_3.

TABLE IV. THE PROPOSED MULTIPLICATIVE INVERSE P_1

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

TABLE V. THE PROPOSED MULTIPLICATIVE INVERSE P_2

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

TABLE VI. THE PROPOSED MULTIPLICATIVE INVERSE P_3

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

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{bmatrix} \begin{bmatrix} y'_0 \\ y'_1 \\ y'_2 \\ y'_3 \\ y'_4 \\ y'_5 \\ y'_6 \\ y'_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \bmod 2 \quad (1)$$

TABLE VII. THE PROPOSED S-BOX$_1$

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

TABLE VIII. THE PROPOSED S-BOX$_2$

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

TABLE IX. THE PROPOSED S-BOX$_3$

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

After S-box$_1$, S-box$_2$, and S-box$_3$ are built, the next step is to test SAC on the three S-boxes. In a mathematical formulation, SAC is defined in the following Equation 2 [6]:

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

where n is the number of variables in GF(2^8) which is 8, and i is the number 1 in the i^{th} position. The ideal value of SAC is 0.5. That is, if there is 1 bit input that changes value, then 4 out of 8 output bits that have changed the value. The closer the value of 0.5, the better the SAC value [16].

TABLE X. THE SAC VALUES OF THE PROPOSED S-BOX$_1$ TO S-BOX$_3$

S-boxes	SAC
S-box$_1$	0.49585
S-box$_2$	0.49585
S-box$_3$	**0.49658**

Based on Table X, S-box$_3$ has a SAC value of 0.49658. SAC value on S-box$_3$ is better than SAC value on S-box$_1$ and S-box$_2$. Thus, the best proposed S-box is proposed S-box$_3$. The SAC proposed S-box$_3$ matrix in detail is shown in Table XI.

TABLE XI. THE SAC MATRIX OF THE PROPOSED S-BOX$_3$

0.453125	0.46875	0.46875	0.5	0.484375	0.5	0.53125	0.515625
0.453125	0.453125	0.515625	0.515625	0.5	0.48438	0.46875	0.53125
0.453125	0.453125	0.5	0.484375	0.5	0.5	0.53125	0.46875
0.515625	0.453125	0.5	0.53125	0.453125	0.5	0.51563	0.53125
0.53125	0.515625	0.546875	0.5	0.484375	0.45313	0.46875	0.515625
0.515625	0.53125	0.515625	0.546875	0.515625	0.48438	0.5	0.46875
0.4375	0.515625	0.453125	0.5	0.546875	0.51563	0.54688	0.5
0.5	0.4375	0.484375	0.484375	0.484375	0.54688	0.45313	0.546875

IV. RESULT AND DISCUSSION

In this section, we will explain the comparison of SAC value result from the proposed method and the SAC values on those produced by previous researchers.

Table XII shows the comparison of SAC values from previous researchers with various methods. Value of SAC AES, in Refs. [7], in Refs. [8], in Refs. [9], in Refs. [10], in Refs. [11], and in Refs. [12] are 0.50488, 0.51074, 0.50659, 0.50635, 0.16309, 0.49300, and 0.5039 respectively. Meanwhile, the SAC value of the proposed S-box is 0.49658. The result of the SAC value from proposed S-box has better value than SAC AES and the other S-boxes.

TABLE XII. THE PERFORMANCE COMPARISON OF SAC VALUES

S-boxes	SAC
Proposed S-box	**0.49658**
AES	0.50488
In [7]	0.51074
In [8]	0.50659
In [9]	0.50635
In [10]	0.16309
In [11]	0.49300
In [12]	0.5039

V. CONCLUSION

The method offered in building the S-box in this paper is the technique of algebra using the selected irreducible polynomial $p_1(x) = x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$, $p_2(x) = x^8 + x^6 + x^3 + x^2 + 1$, and $p_3(x) = x^8 + x^4 + x^3 + x^2 + 1$. From the three irreducible polynomials the multiplicative inverse matrixes p_1, p_2, and p_3 are produced. Furthermore, using affine transforms produces S-box$_1$, S-box$_2$, and S-box$_3$.

The strength of each S-box is tested using SAC. The SAC values of S-box$_1$, S-box$_2$, and S-box$_3$ are respectively 0.49585. 0.49585, and 0.49658. From the comparison of SAC values, it appears that S-box$_3$ is the best S-box compared to S-box$_1$ and S-box$_2$. So, the best proposed S-box is S-box$_3$.

The SAC value of the best proposed S-box compared to the SAC value in the previous researchers turned out to have a better SAC value.

REFERENCES

[1] C. K. Wu and D. Feng, *Boolean Functions and Their Applications in Cryptography*. Springer, Berlin, Heidelberg, 2016.

[2] 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.

[3] J. Daemen and V. Rijmen, *The Design of Rijndael*. Springer-Verlag Berlin Heidelberg New York, 2002.

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

[5] Alamsyah, A. Bejo, and T. Bharata Adji, "AES S-Box Construction Using Different Irreducible Polynomial and Constant 8-bit Vector," in *2017 IEEE Conference on Dependable and Secure Computing*, 2017, pp. 366–369.

[6] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Williams H.C. (eds) Advances in Cryptology — CRYPTO '85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science, vol 218.*, 1986, pp. 523–534.

[7] R. Girija and H. Singh, "Enhancing Security of Double Random Phase Encoding Based on Random S-Box," *3D Res.*, vol. 9, no. 2, p. 15, 2018.

[8] S. Farwa, N. Muhammad, T. Shah, and S. Ahmad, "A Novel Image Encryption Based on Algebraic S-box and Arnold Transform," *3D Res.*, vol. 8, no. 3, 2017.

[9] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-Box," *Chaos, Solitons & Fractals*, vol. 95, pp. 92–101, 2017.

[10] 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.

[11] M. Khan, T. Shah, H. Mahmood, M. Asif, and G. Iqtadar, "A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems," *Nonlinear Dyn.*, vol. 70, pp. 2303–2311, 2012.

[12] Ü. Çavusoglu, A. Zengin, I. Pehlivan, and S. Kaçar, "A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system," *Nonlinear Dyn.*, pp. 1081–1094, 2016.

[13] Alamsyah, A. Bejo, and T. B. Adji, "The replacement of irreducible polynomial and affine mapping for the construction of a strong S-box," *Nonlinear Dyn.*, 2018.

[14] 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.

[15] 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.

[16] C. Adams and S. Tavares, "Good S-Boxes Are Easy To Find," in *Advances in Cryptology — CRYPTO' 89 Proceedings. CRYPTO 1989. Lecture Notes in Computer Science book series, volume 435*, 1990, pp. 612–615.

paper

ORIGINALITY REPORT

9%	3%	9%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

3%

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

Publication

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		