Enhancement strict avalanche criterion value in robust S-boxes construction using selected irreducible polynomial and affine matrixes

Alamsyah¹,² *, A Bejo¹ and T B Adji¹

¹ Department of Electrical Engineering and Information Technology, Universitas Gadjah Mada, Indonesia
² Department of Computer Science, Universitas Negeri Semarang, Indonesia

*Corresponding author: alamsyah.16@mail.ugm.ac.id; alamsyah@mail.unnes.ac.id

Abstract. One indicator that a robust S-box is an ideal strict avalanche criterion value of 0.5. One method for applying the ideal strict avalanche criterion value is the selection of the precise irreducible polynomial and affine matrix. In this paper, we will discuss the robust S-boxes construction with the selected irreducible polynomial \( r(x) = x^8 + x^5 + x^3 + x^2 + 1 \) combined with the three selected affine matrixes i.e. \( t_1 \), \( t_2 \), and \( t_3 \). Hence, the combination of selected irreducible polynomial and affine matrixes results in S-box1, S-box2, and S-box3. The test of strict avalanche criterion shows that S-box2 and S-box3 produce the same value of 0.49951. Nonlinearity and bit independence criterion tests are also conducted to complete the S-box testing. This result shows S-box2 and S-box3 are the best S-boxes compared to S-box1 and S-boxes from previous studies.

1. Introduction

S-box has an important role in the process of data encryption and decryption. The robust of the S-box generated greatly determines the robust of the block cipher algorithm [1] such as data encryption standard (DES) or advanced encryption standard (AES). The main reason for the collapse of the DES algorithm is that the resulting S-box is not strong against linear attack [2,3].

Studies of various types of attacks on block cipher algorithms have been widely presented by previous researchers. The existence of a new variant in a linear attack called affine linear cryptanalysis has been described [4]. An integral attack with a new concept called a new statistical integral distinction can reduce data complexity compared to the previous methods [5]. Research on robust an S-box construction to anticipate linear attacks using the revised genetic algorithm method has been presented [6]. A new concept to calculate the value of a non-linearity of an S-box have been presented [7]. At present, AES S-box is still considered strong against linear, differential, integral and other attacks. However, it is necessary to develop S-box construction that is stronger than the AES S-box to anticipate future attacks.

Strict avalanche criterion (SAC) is a method for measuring the robust of an S-box. The SAC concept was first introduced [8]. SAC is used to observe changes that occur in input bits and output bits. If there is a change in 1-bit input, then ideally there is half of the output bit changed. This means that the ideal SAC value is 0.5 [8]. In addition to SAC, methods for measuring the robust of S-box are nonlinearity [9] and bit independence criterion (BIC) [8].

S-box construction has been carried out by previous researchers with various methods. The double random phase encoding (DRPE) method [10], the iterative map method [11], a random number generating (RNG) method [12], the quantum magnets and Lorenz chaotic system method, Chaotic-
based systems [14-19], and Other methods in building S-boxes [20-26]. Unfortunately, from previous studies [10-26] the optimal value was only obtained in nonlinearity and BIC testing. The SAC value still needs to be improved to produce a strong S-box.

In this paper, we will present S-box construction using selected irreducible polynomial and affine matrixes. This method starts by determining the selected irreducible polynomial that meets in GF(2^8), builds multiplicative inverse, applies affine mapping with selected affine matrixes, and finally constructs an S-box. All S-boxes produced will be tested using SAC, nonlinearity, and BIC. The best S-boxes are the S-boxes that have the best SAC, nonlinearity and BIC values among the proposed S-boxes. The results of SAC, nonlinearity, and BIC from the best S-boxes will be compared with previous studies.

2. Method

2.1. Irreducible polynomial

In this section, we will discuss the irreducible polynomial. An irreducible polynomial is a polynomial that has two multiplication factors, i.e., itself and 1 [27]. To get the irreducible polynomial, the following steps are taken.

Step 1. List all polynomials that meet the following conditions
   1.a. starting from polynomial \(x^8\),
   1.b. finishing until polynomial \(x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1\)

Step 2. Perform division operations with the following conditions
   2.a. starting from polynomial 1
   2.b. finishing until polynomial is running at that time

Step 3. The setting value of the variable \(P = 0\)
Step 4. Each division result in step 2 is equal to 1, adding value 1 to variable \(P\)
Step 5. Calculate the value of the \(P\) variable for each polynomial that meets in step 1
Step 6. If \(P <> 2\), then the polynomial in step 1 is called a reducible polynomial
Step 7. If \(P = 2\), then the polynomial in step 1 is called a irreducible polynomial
Step 8. Show all irreducible polynomials

After Step 1 until Step 8 is run, there are 30 irreducible polynomials that have been classified according to listed in [28], [29], and [30]. Based on 30 irreducible polynomials, the selected irreducible polynomial is \(r(x) = x^8 + x^6 + x^4 + x^2 + 1\). The choice of the irreducible polynomial is based on the computational speed in forming the irreducible polynomial. In accordance with the selected irreducible polynomial, a multiplicative inverse table is constructed as listed in Table 1.

Table 1. The proposed multiplicative inverse

|   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 150 | 228 | 75 | 92 | 114 | 197 | 179 | 67 | 46 | 253 |
| 207 | 247 | 183 | 50 | 23 | 233 | 232 | 20 | 138 | 38 | 30 | 218 |
| 241 | 73 | 237 | 107 | 205 | 186 | 25 | 139 | 157 | 254 | 226 | 249 |
| 69 | 225 | 19 | 182 | 15 | 245 | 109 | 161 | 61 | 12 | 88 | 133 |
| 238 | 143 | 178 | 9 | 224 | 48 | 163 | 243 | 240 | 33 | 93 | 4 |
| 216 | 201 | 127 | 95 | 113 | 137 | 234 | 125 | 58 | 132 | 192 | 102 |
| 180 | 202 | 230 | 220 | 159 | 194 | 91 | 193 | 145 | 121 | 236 | 35 |
| 136 | 84 | 6 | 196 | 44 | 172 | 212 | 128 | 144 | 105 | 28 | 177 |
| 119 | 213 | 209 | 223 | 89 | 59 | 146 | 214 | 112 | 85 | 24 | 39 |
| 120 | 104 | 134 | 215 | 184 | 167 | 2 | 229 | 77 | 155 | 76 | 153 |
| 108 | 55 | 242 | 70 | 169 | 175 | 185 | 149 | 174 | 164 | 210 | 79 |
| 29 | 123 | 66 | 8 | 96 | 203 | 51 | 18 | 148 | 166 | 37 | 204 |
| 90 | 103 | 101 | 158 | 115 | 7 | 110 | 140 | 217 | 81 | 97 | 181 |
| 222 | 130 | 170 | 78 | 118 | 129 | 135 | 147 | 80 | 200 | 27 | 31 |
| 68 | 49 | 42 | 248 | 3 | 151 | 98 | 221 | 22 | 21 | 86 | 124 |
| 72 | 32 | 162 | 71 | 14 | 53 | 206 | 17 | 227 | 43 | 189 | 62 |

2
2.2. Affine mapping

In this section, we will introduce affine mapping. The affine mapping consists of an affine matrix and the addition of a constant 8-bit vector \([31] [32]\) as shown in Eq. (1).

\[
\begin{bmatrix}
    b_0 \\
    b_1 \\
    b_2 \\
    b_3 \\
    b_4 \\
    b_5 \\
    b_6 \\
    b_7
\end{bmatrix}
+ \begin{bmatrix}
    1 \\
    0 \\
    0 \\
    0 \\
    0 \\
    0 \\
    1 \\
    0
\end{bmatrix} \mod 2
\]

(1)

In this paper, we will examine the use of affine matrices based on previous research listed in \([30]\), \([33]\), and \([34]\). The affine matrices are contained as follows:

\[ t_1 = \begin{bmatrix}
    11000001 \\
    11100000 \\
    01110000 \\
    00011100 \\
    00001111 \\
    00000000 \\
    10000000 \\
    11010001
\end{bmatrix}, \quad t_2 = \begin{bmatrix}
    11101001 \\
    11110100 \\
    01111010 \\
    00111101 \\
    10011110 \\
    10111110 \\
    01001111 \\
    11010011
\end{bmatrix}, \quad \text{and} \quad t_3 = \begin{bmatrix}
    01110101 \\
    00111101 \\
    00011110 \\
    10011101 \\
    10100111 \\
    11101001 \\
    11110100 \\
    11110100
\end{bmatrix}.\]

2.3. S-box construction

In this section, we will introduce S-box construction based on selected irreducible polynomial \(r(x) = x^8 + x^5 + x^3 + x^2 + 1\) combined with the three selected affine matrixes i.e. \(t_1\), \(t_2\), and \(t_3\). The S-box construction proposed in detail can be seen in the schematic in Fig. 1. Based on Fig. 1. S-box construction is generated from multiplicative inverse applied to affine mapping transformation. Affine mapping consists of an affine matrix and the addition of a constant 8-bit vector as shown in Eq. (1).

![Affine mapping diagram](image)

**Figure 1.** The construction scheme for the proposed S-box1, S-box2, and S-box3.
Table 2, Table 3, and Table 4 show the results of S-boxes construction based on Fig.1,i.e. S-box1, S-box2, and S-box3, respectively.

### Table 2. The proposed S-box1

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

### Table 3. The proposed S-box2

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

Where $n$ are the number of variables, and $i$ is the number 1 in the $i$th position. Tables 5, 6 and 7 are the results of SAC matrix testing for S-box1, S-box2, and S-box3 respectively.

| Table 4. The proposed S-box1 |
|-----------------------------|
| 99 | 151 | 108 | 105 | 228 | 101 | 102 | 3 | 213 | 67 | 96 | 117 | 225 | 198 | 38 | 97 |
| 77 | 59 | 6 | 91 | 226 | 233 | 29 | 255 | 87 | 199 | 177 | 37 | 193 | 200 | 98 | 209 |
| 1 | 13 | 58 | 122 | 164 | 134 | 127 | 163 | 214 | 104 | 83 | 166 | 92 | 7 | 45 | 129 |
| 121 | 78 | 49 | 242 | 10 | 210 | 64 | 115 | 50 | 23 | 182 | 62 | 227 | 21 | 79 | 188 |
| 39 | 112 | 33 | 48 | 186 | 178 | 154 | 232 | 245 | 9 | 145 | 176 | 24 | 241 | 118 | 61 |
| 204 | 119 | 230 | 120 | 123 | 74 | 244 | 15 | 252 | 202 | 36 | 250 | 68 | 16 | 18 | 12 |
| 27 | 106 | 128 | 31 | 63 | 205 | 171 | 208 | 162 | 220 | 206 | 224 | 135 | 136 | 30 | 153 |
| 190 | 194 | 89 | 247 | 137 | 243 | 184 | 25 | 86 | 147 | 88 | 60 | 0 | 223 | 140 | 248 |
| 65 | 76 | 159 | 2 | 66 | 8 | 191 | 81 | 143 | 54 | 139 | 51 | 234 | 169 | 211 | 170 |
| 40 | 103 | 35 | 165 | 111 | 73 | 138 | 157 | 222 | 236 | 42 | 5 | 156 | 90 | 57 | 19 |
| 180 | 124 | 28 | 100 | 212 | 238 | 155 | 113 | 26 | 84 | 130 | 55 | 168 | 125 | 32 | 160 |
| 172 | 53 | 183 | 196 | 192 | 158 | 175 | 197 | 133 | 189 | 218 | 80 | 219 | 187 | 161 | 85 |
| 95 | 14 | 231 | 203 | 146 | 173 | 93 | 109 | 56 | 229 | 52 | 239 | 114 | 46 | 207 | 44 |
| 246 | 240 | 201 | 195 | 181 | 237 | 215 | 75 | 17 | 131 | 150 | 69 | 221 | 116 | 107 | 4 |
| 141 | 70 | 179 | 82 | 126 | 152 | 41 | 235 | 22 | 11 | 43 | 251 | 142 | 20 | 94 | 132 |
| 249 | 253 | 110 | 144 | 254 | 149 | 185 | 216 | 167 | 71 | 72 | 47 | 148 | 217 | 174 | 34 |

Each S-box produced will be tested using SAC, nonlinearity, and BIC. SAC is defined in Eq. (2) [8] below:

Table 5. The SAC matrix of the proposed S-box1

| 0.5156 | 0.4688 | 0.4844 | 0.5469 | 0.5 | 0.5156 | 0.5156 | 0.5156 |
|-----------------------------|
| 0.5156 | 0.5156 | 0.5 | 0.5469 | 0.5469 | 0.5 | 0.5156 | 0.5156 |
| 0.5156 | 0.5156 | 0.5625 | 0.5156 | 0.5469 | 0.5469 | 0.5 | 0.5469 |
| 0.5469 | 0.5156 | 0.5313 | 0.5 | 0.5156 | 0.5469 | 0.5469 | 0.5313 |
| 0.5313 | 0.5469 | 0.5313 | 0.5469 | 0.5 | 0.5156 | 0.5469 | 0.5 |
| 0.5 | 0.5313 | 0.5156 | 0.5 | 0.5469 | 0.5 | 0.5156 | 0.4531 |
| 0.4531 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5469 | 0.5 | 0.4531 |
| 0.4531 | 0.4531 | 0.5156 | 0.4375 | 0.5 | 0.5 | 0.5469 | 0.5156 |

Table 6. The SAC matrix of the proposed S-box2

| 0.5 | 0.5313 | 0.5156 | 0.5 | 0.5313 | 0.4688 | 0.4688 | 0.5313 |
|-----------------------------|
| 0.5 | 0.4531 | 0.5313 | 0.5625 | 0.5 | 0.5156 | 0.4688 | 0.4844 |
| 0.4531 | 0.5156 | 0.4531 | 0.5156 | 0.5625 | 0.5313 | 0.5156 | 0.4688 |
| 0.5156 | 0.4688 | 0.5156 | 0.4531 | 0.5156 | 0.5156 | 0.5313 | 0.4844 |
| 0.5625 | 0.4375 | 0.4688 | 0.4688 | 0.4531 | 0.4375 | 0.5156 | 0.4844 |
| 0.4844 | 0.5156 | 0.4375 | 0.5313 | 0.4688 | 0.5 | 0.4375 | 0.5 |
| 0.4531 | 0.5 | 0.5156 | 0.5313 | 0.5313 | 0.4688 | 0.5 | 0.5625 |
| 0.5313 | 0.4844 | 0.5 | 0.5313 | 0.5313 | 0.5469 | 0.4688 | 0.5313 |
The results of SAC testing for each proposed S-box are presented in detail in Table 8.

**Table 8.** The SAC values of the proposed S-box\(_1\), S-box\(_2\), and S-box\(_3\)

| S-boxes       | Min  | Mean   | Max  |
|---------------|------|--------|------|
| Proposed S-box\(_1\) | 0.438| 0.51343| 0.563|
| Proposed S-box\(_2\) | 0.438| 0.49951| 0.563|
| Proposed S-box\(_3\) | 0.438| 0.49951| 0.563|

Nonlinearity is defined in Eq. (3) [9] below:

\[
NL (f(x)) = \min d(f(x), g(x)) = \min wt (f(x) \oplus g(x))
\]  

(3)

\(d(f(x), g(x))\) is the Hamming distance to the set of all \(n\)-variable affine functions and \(wt (f(x) \oplus g(x))\) is the number of minterms of \(f(x) \oplus g(x)\). BIC is defined two output bits \(f_i \oplus f_j\) should be highly nonlinear. The results of nonlinearity and BIC testing for each proposed S-box are presented in detail in Table 9.

**Table 9.** The nonlinearity and BIC values of the proposed S-box\(_1\), S-box\(_2\), and S-box\(_3\)

| S-boxes       | Nonlinearity | BIC       |
|---------------|--------------|-----------|
|               | Min | Mean | Max | Min | Mean | Max |
| Proposed S-box\(_1\) | 112 | 112 | 112 | 112 | 112 | 112 |
| Proposed S-box\(_2\) | 112 | 112 | 112 | 112 | 112 | 112 |
| Proposed S-box\(_3\) | 112 | 112 | 112 | 112 | 112 | 112 |

The next section will discuss the performance analysis of each S-box generated in previous studies that will be compared with the best S-box from the results of this research.

**3. Results and Discussions**

Based on Tables 8 and 9, S-box\(_1\), S-box\(_2\), and S-box\(_3\) have SAC values 0.51343, 0.49951, and 0.49951 respectively. The S-boxes have the same nonlinearity and BIC values of 112. Thus, S-box\(_2\) and S-box\(_3\) are selected as proposed S-boxes because the S-boxes have better SAC values. Hence, the proposed S-box\(_2\) and S-box\(_3\) are produced from irreducible polynomial \(r(x) = x^8 + x^4 + x^3 + x^2 + 1\), affine matrix \(t_1\), and affine matrix \(t_2\).

Tables 10 presents the SAC, nonlinearity, and BIC values of the S-boxes that have been presented in previous studies. The SAC, nonlinearity, and BIC values generated from previous studies are varied. But none of the SAC values from previous studies that better than the SAC value 0.49951. Hence, it can be concluded that the proposed S-box\(_2\) and S-box\(_3\) are the best proposed S-boxes because they have SAC value of 0.49951 compared to the SAC value of the S-box resulting from previous studies.
4. Conclusion
In this paper, S-box construction is generated using selected irreducible polynomial $r(x) = x^8 + x^5 + x^3 + 1$ combined with the three selected affine matrices $t_1$, $t_2$, and $t_3$. From the irreducible polynomial, the multiplicative inverse matrix is produced. Furthermore, using affine mapping, S-box1, S-box2, and S-box3 are built. Proposed S-box2 and S-box3 are the best S-boxes in this paper with SAC value of 0.49951. The SAC value of proposed S-boxes is compared to the SAC value of the S-boxes resulting from previous studies. The result are that the proposed S-box2 and S-box3 are the best compared to the available previous S-boxes.

References
[1] Wu C K and Feng D 2016 Boolean Functions and Their Applications in Cryptography (Berlin: Springer) 2016
[2] Biham E and Shamir A 1991 J. Cryptol. 4 3
[3] Paar C and Pelzl J 2010 Understanding Cryptography (Berlin: Springer-Verlag)
[4] Nyberg K 2019 Cryptogr. Commun. 11 367
[5] Cui W, Chen W, Mesnager S, Sun L and Wang M 2018 Cryptogr. Commun. 10 755
[6] Ivanov G, Nikolov N and Nikova S 2016 Cryptogr. Commun. 8 247
[7] Liu J, Mesnager S and Chen L 2017 Cryptogr. Commun. 9 345
[8] A. F. Webster and S. E. Tavares 1986 Lecture Notes in Computer Science 218 523
[9] Hussain I and Shah T 2013 Nonlinear Dyn. 74 869
[10] Girija R and Singh H 2018 3D Res. 9 15
[11] Farwa S, Muhammad N, Shah T, Ahmad S 2017 3D Res. 8 26
[12] Çavuşoğlu U, Kaçar S, Pehlivan I and Zengin A 2017 Chaos, Solitons & Fractals 95 92
[13] Hussain I, Anees A, Al Khalidi A, Algharni A and Aslam M 2018 Chinese J. Phys. 56 1609
[14] Özkaynak F, Çelik V and Özer A B Signal, Image Video Process. 11 659
[15] Özkaynak F and Yavuz S 2013 Nonlinear Dyn. 74 551

Table 10. Performance comparison

| S-boxes     | SAC   | Nonlinearity | BIC |
|-------------|-------|--------------|-----|
| AES         | 0.5048| 112          | 112 |
| In [10]     | 0.5107| 103          | 103 |
| In [11]     | 0.5066| 104          | 103 |
| In [12]     | 0.5064| 106          | 104 |
| In [13]     | -     | -            | -   |
| In [14]     | 0.4956| 105          | 103 |
| In [15]     | 0.5036| 104          | 103 |
| In [16]     | 0.4983| 105          | 104 |
| In [17]     | 0.4976| 106          | 105 |
| In [18]     | 0.4930| 105          | 98  |
| In [19]     | 0.4978| 105          | 104 |
| In [20]     | 0.503 | 107          | 104 |
| In [21]     | 0.503 | 112          | 112 |
| In [22]     | 0.504 | 106          | 103 |
| In [23]     | 0.502 | 106          | 103 |
| In [24]     | 0.498 | 108          | -   |
| In [25]     | 0.5002| 106          | 104 |
| In [26]     | 0.5017| 104          | 103 |
| Proposed S-box2 | 0.49951 | 112         | 112 |
| Proposed S-box3 | 0.49951 | 112         | 112 |
[16] Belazi A, Khan M, El-Latif A A A and Belghith M 2016 Nonlinear Dyn. 87 337
[17] Liu G, Yang W, Liu W Dai Y 2015 Nonlinear Dyn. 82 1867
[18] Khan M, Shah T, Mahmood H, Asif M and Iqtadar G 2012 Nonlinear Dyn. 70 2303
[19] Khan M and Shah T 2015 Signal, Image Video Process. 9 1335
[20] Lambic D 2017 Nonlinear Dyn. 87 2407
[21] Khan and Azam N A 2015 3D Res. 6 1
[22] Çavusoglu U, Zengin A, Pehlivan I and Kaçar S 2016 Nonlinear Dyn. 87 1081
[23] Ullah A, Shaukat S, Tariq J 2017 Nonlinear Dyn. 88 2757
[24] Isa H, Jamil N and Aba M R Z 2016 New Gener. Comput. 7 221
[25] Islam F and Liu G 2017 3D Res. 8 1
[26] Hussain I, Gondal M A and Hussain A 2015 3D Res. 6 1
[27] Stallings 2017 Cryptography and Network Security 7th ed (London: Pearson Publishing)
[28] Gangadaril B R and Ahamed S R 2015 Proc. Eighth Int. Conf. on Contemporary Computing (IC3) (Noida) (New Jersey: IEEE)
[29] Wang D and Sun S L 2008 Proc. Int. Conf. on Computer Science and Software Engineering (Hubei) (New Jersey: IEEE) p 782
[30] Alamsyah, Bejo A and Adj T B 2018 Nonlinear Dyn. 93 2105
[31] Daemen J and Rijmen V 2002 The Design of Rijndael (New York: Springer-Verlag)
[32] Alamsyah, Bejo A and Adj T B 2017 Proc. Int. IEEE Conf. on Dependable and Secure Computing (Taipei) (New Jersey: IEEE)
[33] Sahoo O B, Kole D K and Rahaman H 2012 Proc. 2012 Int. Conf. Adv. Comput. Commun. ICACC (Cochin) (New Jersey: IEEE)
[34] Waqas U, Afzal S, Mir M A and Yousaf M 2015 Proc. - 12th Int. Conf. Front. Inf. Technol. FIT 2014 (Islamabad) (New Jersey: IEEE)