Evaluation of Key Dependent S-Box Based Data Security Algorithm using Hamming Distance and Balanced Output

Balajee Maram K [1], J M Gnanasekar [2]

[1] Research and Development Centre, Bharathiar University, Coimbatore, Dept. of CSE, GMRIT, Rajam, India.
[2]Department of Computer Science & Engineering, Sri Venkateswara College of Engineering, Sriperumbudur Tamil Nadu, India

Abstract: **Data security is a major issue because of rapid evolution of data communication over unsecured internetwork. Here the proposed system is concerned with the problem of randomly generated S-box. The generation of S-box depends on Pseudo-Random-Number-Generators and shared-secret-key. The process of Pseudo-Random-Number-Generator depends on large prime numbers. All Pseudo-Random-Numbers are scrambled according to shared-secret-key. After scrambling, the S-box is generated. In this research, large prime numbers are the inputs to the Pseudo-Random-Number-Generator. The proposed S-box will reduce the complexity of S-box generation. Based on S-box parameters, it experimentally investigates the quality and robustness of the proposed algorithm which was tested. It yields better results with the S-box parameters like Hamming Distance, Balanced Output and Avalanche Effect and can be embedded to popular cryptography algorithms.**

Keyword: **S-BOX, Data Security, Large Prime Number, Random Number, Cryptography.**

DOI: 10.18421/TEM51-11
https://dx.doi.org/10.18421/TEM51-11

Corresponding author: Balajee Maram K: Bharathiar University, India
J M Gnanasekar: Sri Venkateswara College of Engineering, Sriperumbudur Tamil Nadu, India.

1. INTRODUCTION

In digital communication, the data is being captured by hackers [1]. Such type of attacks can be reduced by Data Encryption and Decryption Algorithms [2]. Symmetric-key encryption and Asymmetric-key encryption are two categories of Encryption Algorithms. Symmetric-Key cryptography algorithms are 1000 times faster than the Asymmetric-encryption algorithms [3]. Still, the data is being exchanged in insecure communication channels [4]. The block ciphers such as DES (Data Encryption Standard) [5], AES (Advanced Encryption Standard) [6], and EES (Escrowed Encryption Standard) [7] are popular Cryptography algorithms. The operations XOR, ADD & SHIFT used by the Tiny Encryption Algorithm (TEA) [8,9,10] is one of the fastest and most efficient algorithms.Shannon’s properties confusion and diffusion [9] which are important for a security of block ciphers satisfied in TEA algorithm. But TEA suffers from equivalent keys, because its key size is only 126-bits [11]. The algorithm in [12,13] suggests the traditional cryptography algorithms are not suitable to low processing devices like mobile devices, because low processing devices have slow processor, limited battery and limited memory.

Confusion and Diffusion is an important characteristic for Information Security. S-Box in existing symmetric cryptography algorithms supports Confusion [14]. S-Box is a mapping table which translates data from one form to another. The design and analysis of a strong S-Box is a time consuming process, because it supports nonlinearity to the cryptosystems. The weakness in the design of S-Box is the limitationwhich leads to break easily[15,16]. The S-Box design is being suffered from two major challenges. They are S-Box Searching and Verification of S-Box against the desired properties for an S-Box[17].

S-Box is a nonlinear component which enables that block cipher is resistant to various attacks suchas linear and differential cryptanalysis. This is achieved in Substitution-Permutation(SP) networks when S-Box satisfies the criteria like Avalanche Effect, Strict Avalanche Criteria (SAC) and Bit Independence Criteria (BIC), nonlinearity and maximum expected linear probability (MELP) [18,19] etc. These are the desirable properties for S-Box design[20,21].

For Symmetric encryption/decryption, random key-dependent S-Boxes are being generated for encryption process[18,22,23] and S-Box are generated, then checked until a strong S-Box is found [24], [42]. For Symmetric Encryption, two shared-secret-keys have been used in [25]. Sharing two secret-keys is not an easy task.

According to [26], Cryptography depends on mathematics. Authentication and confidentiality depend on mathematics.

The proposed system is able to handle and solve the limitations in existing light-weight cryptography algorithms. It is based on two large prime numbers for generating Pseudo-Random Numbers. For different seeds (different large primes), it can generate different Pseudo-Random Numbers. The proposed system can use two large primes, bitwise-XOR operation and some mathematical methods to scramble the bits. It is able to handle 512-bit blocks and key. This paper works on the properties like Hamming-Distance, Balanced-Output and Avalanche-Effect.

1.1. Properties of S-box

In particular there are many research papers that applied criterions for making good S-boxes which make the cipher resistant against differential and linear cryptanalysis. Some of the formal design criterions of S-boxes[27] for cryptographic purposes are as follows.

1.1.1 Strict Avalanche Criterion (SAC)

The second important characteristic of any cryptosystem is that Strict Avalanche Criterion (SAC). When there is change in 1-bit of plain-text then it should affect more than half of the bits in cipher-text. Or, when there is a change in 1-bit of key then it should affect more than half of the bits in cipher-text. This is called Avalanche Effect.

1.1.2 HammingDistance

The Hamming distance between two strings of equal length is the number of positions at which the corresponding symbols are different. In another way , it measures the minimum number of substitutions required to change one string into the other, or the minimum number of errors that could have transformed one string into the other.

1.1.3 Balanced Output

Balanced output [27] is the output which has the number of 1's & 0's should be approximately equal.

Finally, there are three requirements regarding the values in the s-box. First, the distributions of outputs must be checked for uniformity to protect against the Davies' Attack. Second, the outputs must have no linearity in their function to the input. Third, there must be unique values in every row of the s-box. There are several other requirements; however they are beyond the scope of this paper.

2. LITERATURE SURVEY

In this section, some of the existing algorithms are presented to discuss:

An algorithm for S-Box generation "*Designing the S Boxes of Blowfish Algorithm using Linear Congruential Generator*" [27] has been proposed. In this paper, the S-BOX generation is based on pi values which lead to easier cryptanalysis. The pi values are replaced with Linear Congruential Generator. This algorithm gives better results than original blowfish algorithm. But the maximum period of Linear Congruential Generator is M-1, which is much too small for 32-bit generators whereM$\leq 2^{32} \approx 10^9$, since this can be exhausted in a few minutes on a workstation.

"*Efficient Implementation of AES by Modifying S-Box*" [28] has been explained. The performance of the original AES algorithm using S-BOX which is based on polynomial is very good. Here, S-box and Inv S-box have been modified by swapping each word of S-box and Invs-box generated by new polynomial. The result shows the modified AES shows better results.

Random S-Box generation algorithms have been proposed and compared in "Comparison of Randoms-Box Generation Methods" [29]. The S-BOX is generated using Legendre's sequences. It shows nonlinearity of generated S-boxes giving the maximum nonlinearity and concludes that it is possible to generate "good" S-boxes.

Dynamic AES-128 with Key-Dependent S-box [30] presents a new algorithm that generates a dynamic AES with key-dependent S-Boxes. A small change in the secret key reflects the structure of the S-Box. In [30], s-box rows and columns are interchangeable which is based on S1 vector and S2 vector. The result shows this algorithm improves the AES security.

Cryptographically strong S-Box is proposed in "*Construction of Cryptographically Strong 8x8 S-boxes*" [31]. The construction of S-box is the action of PGL (2, GF (2^8)) group onGF(2^8); It is comparable with AES S-box, Affine Power Affine S-box, Gray S-box. And it is better than Prime S-box.

In this paper, Key-Dependent S-Box [32] is proposed to generate a dynamic S-Box. This research showed the intensive analysis for cost and security for 1bit, 2bits, 4bits and more than 4 bits. Depending on the application, the suitable method can be selected.

Key-dependent S-box has been proposed in "*Key-Dependent S-Box Generation in AES Block Cipher System*" [33]. The static s-boxes are vulnerable. So the dynamic s-boxes are resistant to different attacks. The proposed system is used to generate large number of s-boxes by changing the secret-key.

A new strategy has been proposed in "*A novel design for the construction of safe S-boxes based on TDERC sequence*" [34] for developing cryptographically strong 8X8 S-boxes. These proposed S-boxes satisfy bijective and nonlinearity properties.

A new S-box was constructed in "*Performance Efficiency of Modified AES Algorithm Using Multiple S-Boxes*" [35] using XOR operation and affine transformation. Here the AES-2SBox was more efficient by 22.986% and 109.79% respectively than the original AES algorithm. From these results, we observed that the speed performance significantly increased in the modified AES algorithm using multiple S-Boxes, while the security side has slightly weakened.

The S-Box Rotation has been added in "*Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key*" [36], and is introduced at the beginning of the round function. This property can be used to make the S-box key-dependent.

A new way of generating the elements in and P arrays and S box has been proposed in [37]. The algorithm offers sufficient resistance towards Brute force attack and statistical crypt analysis of original and encrypted images.

The masked S-box has been proposed in [38] and has the ability to defend against DPA and glitch attacks, thereby offering high security level. The masked S-box maps the plaintext and masking values from GF(2^8) to GF(2^4) and vice-versa. Thus the implementation of masked s-box increases the system security and the algorithm's performance.

A new nonlinear transformation for AES S-box has been presented in [39] which enhance the complexity of the S-box structure. The alignment of the biometrics scheme with AES algorithm provides an additional protection in authentication system.

The concept of using key-dependent s-box manipulations to strengthen specific block ciphers against attacks which depend upon knowledge of the s-boxcontents has been proposed in [40]. Cryptographic strength may be substantially increased with hidden s-box contents.

The important characteristic of a Data Security is Avalanche-Effect. How to improve the Avalanche-Effect is explained in "*Light Weight Cryptographic algorithm to Improve Avalanche Effect for Data Security using Prime Numbers and Bit Level Operations*" [41]. It gives better results than the existing results. It is based on simple mathematical operations and logical methods.

3. PROPOSED/MODIFIED S-BOX CONSTRUCTION

3.1 Pseudo-code for Generation of Pseudo-Random Numbers [43]

Here are generated Pseudo-Random Numbers that are needed for Encryption/Decryption process. The generation process of Pseudo-Random Numbers is as follows:

```
1: Take two large prime numbers p and q.
2: for all i=0, 1, …, 255 do
3: p=(p*q+1) mod 256
4: a(i)←p
5: end for
```

3.2 Pseudo-code for Generation of Random Numbers for positions in S-Box [43]

Here are generated Pseudo-Random Numbers that are needed for positions to keep the Pseudo-Random Numbers in S-box for Encryption/Decryption process. The generation process of Pseudo-Random Numbers for position is as follows:

```
1: Calculate next primes of p and q are p1 and q1
2: for all i=0, 1, …, 255 do
3: p1=(p1*q1+1) mod 256
4: p(i)←p1
5: end for
```

3.3 Algorithm for Generation of Key-Dependent Random S-Box

a)Input:

i) The secret key key[i], i= 1, 2, …, n is the vector of n integer numbers from the interval [0..255].

ii) Array of Random Numbers i.e. a() for S-Box values

iii) Array of RandomNumbers i.e p() for positions

iv) Number of rounds ‘rounds’

b)Output:

i) The key-dependent substitution box S-Box(i)(j), i= 0,1,…,15 and j=0,1,…,15 is the 2-Dimensional vector of the different integer numbers(bytes) from the range [0,255].

ii) The key-dependent inverse substitution box invS-Box(i)(j), i= 0,1,…,15 and j=0,1,…,15 is the 2-Dimensional vector of the different integer numbers(bytes) from the range [0,255].

c)Algorithm:

```
Step 1: Make S-Box(i)(j) from the array a(),i= 0,1,…,15 and j=0,1,…,15 is the 2-Dimensional vector of the different integer numbers(bytes) from the range [0,255].
Step 2: Each row in S-Box()() is circularly shifted to Left/Right according to the values of Key()
Step 3: for round=1 .. rounds do
Step 4: for all row=0, 1, …, 16 do
Step 5: if key(index) is even then row in S-Box()() is circularly shifted to Left of key(index) mod 16 positions
Step 6: if key(index) is odd then row in S-Box()() is circularly shifted to Right. Of key(index) mod 16 positions
Step 7: end of Step 4 for loop
Step 8: end of Step 3 for loop
Step 9: All the elements in S-Box()() are permuted according to values in p() array.
Step 10: Now S-Box()() is ready.
```

Using Pseudo-Random-Number generation algorithm, 256 numbers are generated in the range [0,255]. These 256 numbers are placed in 16X16 2-Dimensional matrix called S-box. Each row in S-box is circularly shifted to Left/Right according to the values of Shared-Secret-Key. If the key(index) is even then the row in S-box is circularly shifted to left of key(index) mod 16 positions. If the key(index) is odd then the row in S-box is circularly shifted to right of key(index) mod 16 positions. The above process will be continued for the given number of rounds. Again Pseudo-Random-Number generation algorithm, 256 numbers are generated in the range [0,255]. These 256 numbers are placed in 1-Dimensional array p(). All the elements in S-Box are permuted according to the values in the array p(). Now the key-dependent S-box is generated and ready to use in Encryption/Decryption process.

3.4 Algorithm for Inverse S-Box [43]

```
Step 1: Arrange all the elements from S-Box()() to a()
Step 2: for all i=0,1,…,255 do
Step 3: Calculate inva(a(i))←i
Step 4: end for
Step 5: Arrange all the elements from inva() to invS-Box()()
Step 6: Inverse of S-Box()() is ready.
```

All the elements in S-box are rearranged from 2-dimensional array to 1-dimensional array ‘a’.The inverse of ‘a’ is calculated using the following formula: Inva(a[index])=index. Then all 256 elements are rearranged from 1-dimensional to 2-dimensioal array called invS-Box.

4. EXPERIMENTAL RESULTS OF THE PROPOSED SYSTEM

In this section the results of analysis are given. The analysis includes the comparison of the properties of S-box like Hamming-distance, Balanced-output and Avalanche Effects of proposed and existing algorithms. The proposed algorithm has been checked through JAVA code.

The shared secret prime numbers are p=7933,q=8161 for first example and p=9901,q=10009 for second example.

4.1 Example1

key[]={65,177,99,34,60,189,222,200,187,155,23,9,13,68,14,0,35,161,171,201,229,254,49,52,90,111,119,117,131,137,129,163,217,229,246,65,177,99,34,60,189,222,200,187,155,23,9,13,68,14,0,35,161,171,201,229,254,49,52,90,111,119,117,131,137};

PRIME NUMBERS: p=7933,q=8161

PLAIN-TEXT: “cryptography”

Table 1: Elements in S-BOX of 4.1

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

From Table 1, there is no relationship between any two consecutive rows. In each row, there is no relationship between any two consecutive elements. Hence it is not possible to predict the elements in an S-box.

Table 2: Elements in Inverse S-Box of 4.1

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

From Table 2, there is no relationship between any two consecutive rows. In each row, there is no relationship between any two consecutive elements. Hence it is not possible to predict the elements in Inverse S-box.

<u>OUTPUT</u>: ?¥$ƒISáH$xIƒ

4.2 Avalanche Effect using S-boxof4.1

An S-box satisfies SAC if a single bit changes on the input results in a change on a half of output bits. Note that when S-box is used to build an S-P network, then a single change on the input of network causes an avalanche of changes.

Table 3: Avalanche effect OF A...Z Using S-boxof Table 1

Actual Data	65	66	67	68	69	70	71	72	73	74	75	76	77
	78	79	80	81	82	83	84	85	86	87	88	89	90
Avalanche Effect(%)	62.5	62.5	75	75	62.5	62.5	62.5	75	75	50	50	50	50
	50	50	37.5	37.5	37.5	50	50	50	62.5	62.5	75	75	50

From Table3, weconclude that the Avalanche Effect of alphabets (A to Z) in the proposed system is very effective. In proposed system, change in 1-bit reflects half or more than half of the bit in the output. In the best case, the Avalanche Effect is 75%. In the worst case, the Avalanche Effect is 50%. The Avalanche Effect of the alphabets (A to Z) is in the range 50% to 75%. The Average is 57.69231.

4.3 Example 2

key[]={65,177,99,34,60,189,222,200,187,155,23,9,13,68,14,0,35,161,171,201,229,254,49,52,90,111,119,117,131,137,129,163,217,229,246,65,177,99,34,60,189,222,200,187,155,23,9,13,68,14,0,35,161,171,201,229,254,49,52,90,111,119,117,131,137};

PRIME NUMBERS: p=9901,q=10009

*Table 4: Elements in S-BOXof 4.*3

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

5. DISCUSSION ON SECURITY PARAMETERS

5.1 Security Analysis

The privacy of data is measured by the variance between the actual and the perturbed values which is given by the following formula:

$$A=\frac{\mathrm{VAR}\,(A-A')}{VAR\,(A)}$$

Table 5: Before S-BOX & After S-BOX

Before S-Box	99	114	121	112	116	111
	103	114	97	112	104	121
After S-Box	165	36	131	73	83	225
	72	36	120	73	157	131

Table 5 shows the security performance of the proposed system. It compares the data before applying S-box and after S-box. Each element is scrambled through S-box. It has been analyzed that the privacy or the security level of the confidential data is improved a lot by the proposed method.

5.2 Hamming Distance

The Hamming distance between two strings of equal length is the number of positions at which the corresponding symbols are different.

TABLE 6: HAMMING DISTANCE OF PI, LCG AND PROPOSED ALGORITHMS

DATA	C1	C2	C3	C4
RJ45JACK	26	35	32	37
FUNCTION	28	29	37	34
FRAGMENT	25	33	34	34
ZXQRASPK	28	31	37	27
INVERTER	28	32	37	36
ELECTRON	31	31	38	40

Here, C1→ Pi
C2→ LCG
C3→ Proposed Alg. With p=7933,q=8161
C4→ Proposed Alg. With p=9901,q=10009

From Ref [2], the Hamming Distance using pi and LCG is shown in Table 6. The Table 6 shows the Hamming Distance of different strings using proposed algorithms. The Table 6 concludes that the Hamming Distance of the proposed algorithm is best in 4 cases from 6 samples. The Hamming Distance using pi and LCG [2] is less than the Hamming Distance of proposed system. From 6 samples, the proposed system is best in 5 cases.

5.3 Balanced Output

Balanced output is the output which has nearly equal number of 1's & 0's.

TABLE 7: BALANCED OUTPUT OF PI, LCG AND PROPOSED ALGORITHMS

DATA	C1	C2	C3	C4	C1	C2	C3	C4
	0'S				1'S			
RJ45JACK	37	30	32	27	27	34	32	37
FUNCTION	29	32	27	30	39	32	37	34
FRAGMENT	31	31	30	30	33	33	34	34
ZXQRASPK	29	30	27	37	35	34	37	27
INVERTER	32	26	27	28	32	38	37	36
ELECTRON	36	34	26	24	28	30	38	40

Here, C1→ Pi
C2→ LCG
C3→ Proposed Alg. With p=7933,q=8161
C4→ Proposed Alg. With p=9901,q=10009

The total number of 0's and 1's are not synchronized of the Balanced Output in [2]. Here Table 7 concludes that the Balanced Output of the proposed Algorithm is good, because 0's and 1's are synchronized than in existing algorithms [2]. From Table 7, the total number of 0's and 1's are synchronized in the proposed system.

5.4 Avalanche Effect

The proposed algorithm is compared with existing algorithms. The proposed algorithm's Avalanche Effect is 75% (Maximum cases). The average value of proposed algorithms is more than 57%.

Table 8: List of algorithms with Avalanche Effect (%)

Encryption Technique	**Avalanche Effect (%)**
This Proposed system (Average case)	**57.69231**
Algorithm in Ref 42	56
DES	54.68
Algorithm in Ref 43	53
AES-RC4	52.34
Algorithm in Ref 44	52.34
Algorithm in Ref 45	49.21
Original AES	46.88
Algorithm in Ref 46	46
Ref 37	44.01
Ref 29	41 to 61
MTEA	32
Blowfish	28.71
TEA	25
Ref 36	24.219
Playfair Cipher	6.25
Vigenere Cipher	3.13
Caesar Cipher	1.56

From Table 8, the Architecture of the proposed system in [22] is not simple and its Avalanche Effect is 56%. According to Table 3, the Avalanche Effect of classical cryptography algorithms is very less (29,37,43,44,45,46). Table 8 concludes the Avalanche Effect of proposed system is the best. The Avalanche Effects are 75%, 37.5%, 57.69% in best-case, worst-case and average-case respectively in proposed system.

6. CONCLUSION

The result shows that a good S-BOX does not depend on the method of generation. Using existing S-BOX generation algorithms consumes more time to generate S-BOX. But in this research paper, a new S-BOX has been proposed which is based on Pseudo-Random generator. It compares the results of Hamming Distance, Balanced Output and Avalanche effect. The proposed S-BOX generation algorithm consumes very less time than the existing algorithms. The total number of 1's and 0's is balanced and Hamming distance between the words also good than existing algorithms. The proposed system can generate 8X8, 16X16 S-BOX. It can be observed that the proposed algorithm offers high encryption quality with minimal memory requirement and computational time. The proposed system is better in terms of Hamming Distance, Balanced Output and Avalanche Effect. So it concludes that we can make use of proposed S-BOX for secure digital communication.

REFERENCES

[1] Stallings W, “Network Security Essentials (Applications and Standards)”, Pearson Education: USA, 2004, pp.2-80.

[2] Pfleeger C P, Pfleeger S L, “Security in Computing”, Pearson Education: USA, 2004, pp. 642-66.

[3] Lecture Notes on “Computer and Network Security” by AviKak.Pdf http:// junicholl.org/Crypt analysis /Data / EnglishData.php, January, 2015

[4] Dragos T, “Sequential and Parallel Cascaded Convolution Encryption with Local Propagation: Toward future Directions in Cryptography,” Proceedings of The third International Conference on Information Technology-New Generations. (ITNG'06), 2006,Las Vegar, NV,(2006), pp.464-69.

[5] Data Encryption Standard: http://csrc.nist. gov/publications/fips/fips46-3/fips- 46-3.pdf, January, 2015

[6]Advanced Encryption Standard: http://csrc.nist.gov/publications/fips/fips197/ fips- 97.pdf, January, 2015

[7]Escrowed Encryption Standard: http://csrc.nist.gov/publications/fips/fips1185/ fips-185.txt, January, 2015

[8] Hernández J C, Isasi P, Ribagorda A, "An application of genetic algorithms to the cryptoanalysis of one round TEA". Proceedings of the 2002 Symposium on Artificial Intelligence and its Application,2002.

[9] Hernández J C, Sierra J M, Isasi P, Ribargorda A,"Finding efficient distinguishers for cryptographic mappings, with an application to the block cipher TEA". Computational Intelligence, 2004, 20(3),pp.517-25.

[10] HernándezJ C, SierraJ M, Ribagorda, A, Ramos B, Mex-Perera J. C. ,"Distinguishing TEA from a Random Permutation: Reduced Round Versions of TEA Do Not Have the SAC or Do Not Generate Random Numbers”,Cryptography and Coding, Springer-Verlag: Berlin Heidelberg, 2001,pp. 374-77.

[11] Kelsey J, Schneier B, Wagner D, "Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X NewDES, RC2, and TEA". Lecture Notes in Computer Science, 1997, ISBN:3-540-63696-X, pp.233–46.

[12]Gupta V, Gupta S, “Securing the Wireless Internet”, IEEE Communications Magazine, 2001,39(12), pp. 68-74.

[13]Daswani N, Boneh D, “Experimenting with Electronic Commerce on the Palm Pilot”, Proc. Third International Conference FC'99, Anguilla British West Indies,Springer Verlag-Berlin Heidelberg, 1999, pp. 1-16.

[14] Mar P P, Latt K M, New analysis methods on strict avalanche criterion of S-boxes, World Academy of Science, Engineering and Technology, 2008,2(12), pp.899-903.

[15]Adams C, Tavares S, The structured design of cryptographically good S-boxes, Journal of Cryptology, 1990,3(1),pp.27-41.

[16] Hussain I, Shah T, Mahmood H, Afzal M, Comparative analysis of S-boxes based on graphical SAC, International Journal of Computer Applications, 2010, 2(5), pp.1-7.

[17] Ahmed N, Testing an S-Box for Cryptographic Use, International Journal of Computer and Electrical Engineering,pp.1-5.

[18] Keliher L,Meijer H, Tavares S, A new substitution-permutationnetwork cryptosystem using key-dependent s-boxes, In: Proc. SAC'97, Canada, (1997),pp.13–26

[19]Keliher L, Refined analysis of bounds related to linear and differential and linear cryptanalysis for the AES, (In: H. Dobbertin et al., eds. Advanced Encryption Standard AES Š04, Bonn, 2004, pp.42–57

[20] Vergili I, Yücel M D., On Satisfaction of Some Security Criteria for Randomly Chosen S-Boxes, in Proc. 20th Biennial Sympisum on Communications, Kingston, 2000, pp.1-5.

[21] Vergili I, Yücel M D, Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen n ×n S-Boxes, Turk Journal of Electrical Engineering, 2001,9(2), pp. 137-45.

[22] Kazlauskas K, Key-dependent S-box generation in AES block cipher system, Informatica,2009,20(1),pp.23–34

[23]Schneier B, Description of a new variable-length, 64-bit block cipher (Blowfish), (In: Proc.Fast Software Encryption, Springer-Verlag:Berlin Heidelberg, , 1994, pp. 191–204

[24]Mroczkowski P, Generating Pseudorandom S-Boxes– a Method of Improving the Security of Cryptosystems Based on Block Ciphers, Journal of Telecommunications Information Technology,2009, pp.74–79.

[25] RAMALINGAM S, Sharmila B S I, Symmetric Encryption Algorithm to Secure Outsourced Data in Public Cloud Storage, Indian Journal of Science and Technology,2015,8(23),pp.1-5.

[26] P. M. DURAI RAJ VINCENT, SYED AMBER IQBAL, KARAN BHAGAT, KAMAL KANT KUSHWAHA, CRYPTOGRAPHY: A MATHEMATICAL APPROACH, Indian Journal of Science and Technology,2013, 6(12),pp.5607-11.

[27] Halagali B P, Hallappanavar V L, Desai V V, Designing The S Boxes of Blowfish Algorithm using Linear Congruential Generator, ASM's International e-journal of Ongoing Research in Management and IT,2013,pp.1-13.

[28] Hallappanavar V L, Halagali B P, Desai V V, Efficient Implementation of Aes By Modifying S-Box, IOSR Journal ofComputer Science (IOSR-JCE), 2014,pp. 35-39.

[29]Mroczkowski P, Generating Pseudorandom S-Boxes, a Method of Improving the Security of Cryptosystems Based on Block Ciphers, Journal of Telecommunications and Information Technology, 2009, pp.74-79.

[30]Mahmoud E M, Abd A,Hafez E, Elgarf T A, Zekry A, Dynamic AES-128 with Key-Dependent S-box, International Journal of Engineering Research and Applications (IJERA), 2013,3(1), pp.1662-70.

[31] Hussain I, Shah T, Gondal M A,Khan W A, Construction of Cryptographically Strong 8x8 S-boxes, World Applied Sciences Journal, 2011, 13 (11), pp.2389-95.

[32] ALDABBAGH S S M, FAKHRI I, Al Shaikhli T, Reza M, ZABA, Key-Dependent S-Box in Light Weight Block Ciphers, Journal of Theoretical and Applied Information Technology, 2014,62(2), pp.554-59.

[33] Kazlauskas K, Kazlauskas J, Key-Dependent S-Box Generation in AES Block Cipher System, Informatica, 2009,20(1),pp.23–34

[34]Alkh aldi A H, Hussain I, Gondal M A, A novel design for the construction of safe S-boxes based on TDERC sequence, Alexandria Engineering Journal,2015,54(1),pp.65-69.

[35] Wenceslao F V, Performance Efficiency of Modified AES Algorithm Using Multiple S-Boxes, International Journal of New Computer Architectures and their Applications (IJNCAA), 2015,5(1), pp.1-9.

[36] Juremi J, Mahmod R, Sulaiman S, Ramli J, Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key, International Journal of Cyber-Security and Digital Forensics (IJCSDF),2012, 1(3),pp.183-88.

[37] Chandrasekaran J, Subramanyan B, Raman G.S, Ensemble of Blowfish With Chaos Based S-Box Design For Text and Image Encryption, International Journal of Network Security & Its Applications (IJNSA), 2011,3(4),pp.165-173

[38] Lekshmi R, Xavier S, FPGA Based Design of AES with Masked S-Box for Enhanced Security, International Journal of Engineering Science Invention,2014,3(5), pp. 01-07.

[39] Vinoth John Prakash S,Arun A, A Secure Software Implementation of Nonlinear Advanced Encryption Standard, IOSR Journal of VLSI and Signal Processing (IOSR-JVSP) 2013,1(5),pp. 44-48.

[40] Harris S, Adams C, Key-Dependent S-Box Manipulations, 5th Annual International Workshop, SAC'98, 1999, Springer-Verlag: Berlin Heidelberg, 1999,pp.15-26.

[41] Balajee Maram K, J M Gnanasekar, Light Weight Cryptographic algorithm to Improve Avalanche Effect for Data Security using Prime Numbers and Bit Level Operations, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 21 (2015) pp 41977-41983.

[42] Cvetanovic, S., Nedic, V., & Eric, M. (2014). Information Technology as A Determinant of SMES Collaboration and Innovativeness. *International Journal for Quality Research*, *8*(4).

[43] Balajee Maram K, J M Gnanasekar,Generation of a Dynamic Random 16X16 S-Box for Unicode Text Using Prime Numbers and Secret-Key, Australian Journal of Basic and Applied Sciences, ISSN: 1991-8178, 9(36), December 2015, pp 140-149.