Iraqi Journal of Statistical Science (29) 2019
Special Issue:First Student Conference
pp[91- 104]

A Review of Block Cipher's S-Boxes Tests Criteria

Dr.Auday H. Saeed AL-Wattar*
Ahsa.alwattar@uomosul.edu.iq

Abstract

The Symmetric Block cipher is a considerable encryption algorithm because of its straightforwardness, rapidity and strength and this cryptographic algorithm is employed in carrying out the encryption and decryption for most current security applications. The confusion properties are attained using the substitution-Box (S-Box). Substitution and permutation functions are normally used in block ciphers to make them much firmer and more effectual ciphers. The Security of S-Box is checked using S-Box test criteria and the randomness test. The objective of this paper is to give the researchers a specific knowledge (standards) for testing the ciphers' S-Boxes. This paper includes survey or guide for the S-box test criteria.

Keywords: Cryptography, Symmetric block cipher, S-Box

استعراض معايير فحص صناديق الاستبدال للتشفير المقطعي

المستخلص

يعتبر التشفير المقطعي المتناظر من خوارزميات التشفير المهمة جدا وذلك بسبب البساطة والسرعة والقوة التي تتميز بها حيث ان خوارزمية التشفير هذه تستخدم في انجاز التشفير وفك الشفرة لاغلب التطبيقات الحديثة. ان خاصية الارباك او الخلط من الممكن الحصول عليها بواسطة استخدام صناديق الاستبدال المسماة (S-Boxes) .

تستخدم وظائف الاستبدال والتشكيل بشكل شائع في خوارزميات التشفير المقطعي لجعلها أكثر صعوبة وفعالية. ان امنية صندوق الاستبدال يتم فحصها او اختبارها باستخدام معايير اختبار صناديق الاستبدال الخاصة إضافة الى اختبار العشوائية. ان الهدف من هذه البحث هو إعطاء الباحثين معرفة محددة (معايير) لاختبار صناديق الاستبدال (S-Boxes). الخاصة بالتشفير المقطعي حيث تتضمن هذه الورقة مسحًا أو دليلًا لمعايير اختبار صندوق الاستبدال (S-Box).

Lecturer / Dept. Computer Science / Computer Science and Mathematics collage / Mosul University

Received Date:29/4 /2019 —— Accepted Date: 8 /7 / 2019

1.0 Introduction

A block cipher converts plaintext blocks of a specific length into ciphertext blocks of the same size affected by a cipher key k; it is a set of Boolean permutations employed on n-bit vectors. This set includes a Boolean permutation for each value of the cipher key k. If the number of bits in the cipher key is denoted by k, a block cipher comprises of 2^k Boolean permutations (Daemen and Rijmen 2002). Block ciphers are frequently known as the work horses of cryptography, and they provide the strength of current protected communication .

Generally, block ciphers are stated by an encryption algorithm, as the sequence of transformations to be implemented in the plaintext to obtain the ciphertext. These transformations are processes with a comparatively simple specification. The generating Boolean permutation relies on the cipher key, based on the fact that key substance, evaluated from the cipher key, is used in the transformation. Block cipher should meet two demands to achieve its goals and these are security and efficiency.

Data or messages to be encrypted are usually termed as plaintext and referred to as (p), which, is represented by blocks of equal sizes of bits, These blocks, in addition to the key k are input to the encryption algorithm (E), and typically E is a set of rounds that work on the plaintext and the key producing the output ciphertext (C) as equal-sized blocks of encrypted data in indecipherable form.

$$C = E_k(p) \text{ or } C = E(p,k) \qquad (1)$$

The decryption process (D) takes the ciphertext in the form of equal sized blocks (C) and the key k as an input performing almost the same set of rounds of encryption, but in reverse order; and the output of the final round are equal sized blocks of the original plaintext (p). This is clearly shown as:

$$p = {E_k}^{-1}(C) \qquad (2)$$

As seen from the term, decryption process is the inverse of encryption process which can be expressed by E^{-1}.

In today's information networks the block ciphers have many benefits since they can be easily regularized and regularly treated and passed on as blocks, thus making the synchronization easier in such a way that losing one block of the ciphertext will not affect the decryption process for the next block.

The defect block cipher does not conceal the input patterns, which are indistinguishable plaintext blocks that are shown as indistinguishable ciphertext blocks (Lai 1992). This weak point was addressed by using the block cipher modes, and this step treatment requires a small amount of memory for the encryption process (Standard 1977).

These Block ciphers are intended to grant data confidentiality by splitting a secret between communication blocks and converting plaintexts to ciphertexts using this secret in a manner that the adversary (having no information of the secret) is not able to attain the plaintext.

A block cipher can be represented as the function:

$$E : F_2^n \times F_2^k \rightarrow F_2^n \qquad (3)$$

These are equivalent to:

$$E: \{0,1,\}^k X\{0,1,\}^n \rightarrow \{0,1,\}^n$$

It is clear from the notation that that E gets two inputs, and gives one output. The two inputs are k-bit and n-bit strings representing the key and the plaintext respectively, while the output is n-bit string which represents the ciphertext. The key-length k and the block length n are two parameters related to the block cipher, the parameters of which differ from one block cipher to another. According to the above the block cipher can be considered as a keyed permutation.

The design of encryption algorithms should be succinct and obvious to satisfy the Kerckhoff principles so as to make the cryptography algorithms more commercialized and thus, the generated algorithm for the cipher should be secure and simple. Diffusion and confusion are two concepts that the symmetric block cipher should possess (Knudsen and Robshaw 2011).

In 1949, Shannon declared the diffusion and confusion as the two basic characteristics to obliterate the wordiness in a plaintext message (Shannon 1949a).

Confusion

Confusion is defined as hiding the relation between the private key and the ciphertext. This indicates that the secret key does not refer in a simple manner to the ciphertext (Coskun and Memon 2006). This means it complicates the relationship between ciphertext and key as much as possible (William and Stallings 2006). It is considered as a first feature in generating a block cipher. The fine confusion means that the relationship statistics is so intricate that even a high degree of cryptanalysis would not succeed.

Confusion property can be supplied using non-linear transformation where the output is not straightforwardly corresponding to its input and each input bit is replaced by another output bit. The most well-known non-linear transformation is the substitution box (S-Box), which can be considered as a small substitution cipher.

The S-Box can be expressed as n × m substitution function, as n and m are not inevitably identical, and they could or could not be equal. Some S-Boxes are invertible while others are not
Confusion property can be supplied using non-linear transformation where the output is not straightforwardly corresponding to its input and each input bit is replaced by another output bit. The most well-known non-linear transformation is the substitution box (S-Box), which can be considered as a small substitution cipher.

S-Boxes

The S-Box represents the significant part of non-linear transformation. For symmetric-key cryptographic algorithms which depend on substitution-permutation (S-P) networks the robustness of the cryptosystem depends to a large extent on the quality of the S-Boxes as poor S-Boxes can lead to weak cryptosystems. (Shannon 1949b).
The S-Box (substitution Box) is considered as a fundamental part since it represents the only non-linear component of symmetric encryption algorithms, that performed substitution (Kazlauskas and Kazlauskas 2009). Regularly, the cipher employs the S-Box to form the combination of the key and the cipher, which is termed confusion as claimed by Shannon (Braeken 2006). Based on the aforementioned, it is clear that the proper design of the S-Box can lead to an increase in the degree of cipher security and one of the very serious aspects in the assessment of the cipher security (Adams and Tavares 1990; Cui and Cao 2007; law Szaban and Seredynski).

2.0 S-Box tests criteria

The designing S-Box should satisfy these criteria in order to make the cryptosystem secure against possible attacks, particularly from linear and differential cryptanalysis.

There are several standards that the S-Boxes should fulfill to be deemed as being a perfect S-Box.

An n × n square S-Box S: $\{1,0\}^n \rightarrow \{1,0\}^n$, which convert a feed in vector X another vector Y, where $X = [x_{n-1}, x_{n-2}, \ldots, x_1, x_0]$, and $Y = [y_{n-1}, y_{n-2}, \ldots, y_1, y_0]$: $Y = S(X)$. Such S-Box S can be defined as 2^n bit numbers, classify $r_{0,\ldots,} r_{2^n-1}$ .In this state $S(X) = [\, C_{n-1}(X), C_{n-2}(X), \ldots, C_0(X)]$, as C_i represent fixed Boolean functions such that $C_i: \{0,1\}^n \rightarrow \{0,1\}$: ∀ i = (0,n-1); which exemplify the S-Box's columns.

A. Balanced

W is a binary vector by n elements such that its coordinates are bits from a set {0,1}

$W = [w_{n-1}, w_{n-2}, \ldots, w_{1,} w_0]$, where $w_{n-1}, w_{n-2}, \ldots, w_{1,} w_0 \in \{0,1\}$.

A Boolean function f: (!!! INVALID CITATION !!!)^{n} → {1, 0} is considered balanced if its truth table has 2^{n-1} ones or zeros:

$$\sum_{W \in \{0,1\}^n} f(W) = 2^{n-1} \qquad (4)$$

S-Box S:$\{0,1\}^n \rightarrow \{0,1\}^n$ is balanced, if and only if when all columns are balanced:

$$\underset{0 \le j \le n-1}{\forall} \quad \underset{\substack{\underline{\propto} \in \{0,1\}^n \\ w(\underline{\propto}) = 1}}{\forall} \quad \sum_{X \in \Sigma^n} f_i\,(X) \oplus f_i(X \oplus \underline{\propto}) = 2^{n-1} \qquad (5)$$

So, if the S-Boxes hold the equivalent number of zeros and ones, it shows that they are balanced, which is one of utmost significant properties of an S-Box.

B. Completeness

The S-Boxes are considered as complete if each output bit hinges on all of the feed in bits by (Webster and Tavares 1986). Y is deemed complete if there is leastwise one couple of plaintext vectors (z and zi), such that:

$(\, z$ and $z_i\,)$ and, $Y(z)$and $Y(z_i)$differ leastwise in bit h, for whole $\{i, h : 1 \le i, h \le n\}$.

In other expression: A Boolean function $f: \{0,1\}^n \rightarrow \{0,1\}$ is consider complete if its output is depend on all its inputs bits, such that its algebraic normal form contains all elements of the input vector $X = [x_{n-1}, x_{n-2}, \ldots, x_{1,} x_0]$.

An n × n square s-box S: $\{1,0\}^n \rightarrow \{1,0\}^n$ is consider complete, if for all vectors,
$A = [a_{n-1}, \dots, a_1, a_0] \in \{0,1\}^n$ *which hamming wight is* 1, hw (A) = 1, there exists vector $W = [w_{n-1}, w_{n-2}, \dots, w_1, w_0] \in \{0,1\}^n$, such that S(W) and S(W⊕A) are dissimilar on bit i for all i ∈ {n-1,…,1,0}.
where the hamming weight hw of a binary vector W, described as hw(W), represents the number of ones within this vector or the number of ones it contains as:

$$hw(W) = \sum_{i=0}^{n-1} wi \tag{6}$$

C. Avalanche criterion

The effect of this is a tremendously desirable characteristic of block ciphers hang out with the computing of diffusion. typically, a block cipher is take into consideration to expose the avalanche effect if for a sole alteration in a single bit of the feed in, the output differs radically (Feistel 1973; Feistel, et al. 1975; Webster and Tavares 1986).
These relevancies could be defined by confirmed terms:
$C_u$is A Vector, that all its elements are 0s, except for one bit *i*, with the value 1.
AV^{C_u} is a vector of avalanche denoting a variance within the production string represent an outcome for the changing of the bit (i) in the feed in text.

$$AV^{C_u} = \mathrm{Y(y)} \oplus \mathrm{Y(y} \oplus \mathrm{c_i}) = \mathrm{av_1^{cu}\, av_2^{cu} av_3^{cu} \dots\, av_m^{cu}} \tag{7}$$

Properly, the criterion of avalanche can be exemplified as:

$$\mathrm{S:}\ \{0,1\}^m \rightarrow \{0,1\}^m$$

It fulfills the Avalanche criterion, if single bit of feed in is completing, typically, bisected of the production bits change.
(S) is considered to fulfill the criterion of avalanche just if for every single u∈(1,...,2^m): where S is a square S-Box with m × m.

$$\frac{1}{2^m} \sum_{v=1}^{m} W(av_v^{c_u}) = \frac{m}{2} \tag{8}$$

In such way that (u, v) stand for feeds in, and products bits, correspondingly, As u, v ∈(1...2^m); and,

$$W(av_v^{c_u}) = \sum_{all\ x \in \{0,1\}^n} (av_v^{c_u}) \tag{9}$$

$$Avalanche\ Effect = \frac{1}{m2^m} \sum_{v=1}^{m} W(av_v^{c_u}) = 0.5 \tag{10}$$

The amount of avalanche must be between the values 0 and 1. The resulted value of the avalanche is 1/2, which indicates that (S) fulfils the avalanche criterion. Though, it is like better to consider the error interval {-∈A,+ ∈A} into consideration for the test consequences (Vergili and Yücel 2001).

Also, the avalanche of the transformation function (S-Box) can be obtained by using the following evaluation (Ramanujam and Karuppiah 2011):

$$Avalanche\ Effect = \frac{Number\ of\ flipped\ bits\ in\ (output) ciphertext}{Number\ of\ All\ bits\ in\ the\ (output) ciphertext}$$

D. Strict avalanche (SAC)

As stated by A. Webster and S. E. Tavares (Webster and Tavares 1986) the S-Box fulfills the criterion of strict avalanche in case that each bit of its products bits is altered by a possibility of single half when a one bit of its products is completed. This standard combine both the avalanche and completeness criteria.

S: $\{0,1\}^t \rightarrow \{0,1\}^t$ for all $d, e \in (1,2,\dots.t)$, fulfills the SAC

If completing single feed in bit *d* varies the product bit *e* by the probability of exactly single bisection (Webster and Tavares 1986).

The S-Box guarantees the SAC in state:

For all d, e

$$Strict\ Avalanche\ Effect = \frac{1}{2^t} W\left(av_e^{c_d}\right) = 0.5 \qquad (11)$$

E. Non-linearity

it is the amount of space amidst the function in matter and the adjacent function which is leaner (Canteaut and Videau 2005; Meier and Staffelbach 1990; Pieprzyk and Finkelstein 1988; Webster and Tavares 1986).

A function F: $F_2^n \rightarrow F_2^m$ As F: $\{0,1\}^n \rightarrow \{0,1\}$

And G (d) is a Boolean function such as G (d) ∈ BFn over F_n^2

$$w_G(d) = \sum_{d \in F_2^n} (-1)^{f(d) \oplus [d,v]} \qquad (12)$$

Where w_G is Walsh transformation of G(d)

The nonlinearity for a function F named S can be expressed as:

$$NL(G) = 2^{n-1} - \frac{1}{2} \max_{d \in F_2^{n*}} |WG(d)| \qquad (13)$$

Stands for the function nonlinearity of the G(*d*) ∈ Bft by utilize the transformation of Walsh, and because n is the function f(*d*) we gain $2^{t-1} - 2^{\frac{t}{2}-1}$ as highest nonlinearity (Carlet and Ding 2007; Gao, et al. 2012).

The non-linearity of G can be defined as the lowest value of the nonlinearities for the whole nonzero linear collections of the constitutive functions.

$$\mathrm{NL(G)} = \min \quad \underset{z \in \frac{F_2^m}{\{0\}}}{\mathrm{Max}} \; \mathrm{NL([z,F]} \qquad (14)$$

Where G is a (n,m) S-Box

F. Bit independency (BIC)

it was stated by as standard employed to examine the security of the produced S-Boxes.

A function $f: \{0,1\}^t \rightarrow \{0,1\}^t$ such that all d,v,y ∈ $(1,2, \dots .t)$, as y ≠ l, fulfils the criterion of bit independence if completing feed in bit *d* forms the production bits e with l to overturn autonomously.

The BIC needs a Corr of the d and v bits for the AV^{c_d}

$$BIC\left(a_e, a_y\right) = \underset{1 \le d \le t}{max} \left|Corr(a_v^{ed}, a_y^{ed})\right| \qquad (15)$$

So, the BIC of S-Box S can be expressed as:-

$$BIC(S) = \underset{1 \le v,y \le t}{max} \; BIC(ad, ay) \qquad (16)$$

Usually the amounts of it can be within 0 and 1 such:

0: The perfect occurrence is totally independent in the connection amid v and y bits.

1: the inferior occurrence is totally dependent on the connection amid v and y bits.

G. Differential uniformity $\delta(G)$

According to (Cui, et al. 2011) the $\delta(S)$ can be represented by

$$\delta(G) = \max_{\substack{\alpha \in F_2^n \\ \beta \in F_2^n \\ \alpha \neq 0}} |\{x | G(x) + G(x+\alpha) = \beta| \qquad (17)$$

As: $G(x) = (g(x), \dots, g_n(x))$, is a multiple product Boolean function of $F_2^n \rightarrow F_2^n$.

The lowest value for δ(G) = 1, the small amount of δ(G) indicates it has a good reluctant against differential attack (Gong, et al.).

H. Invertability

The S-Box fulfils the invertability states, if:

G (x_1) = G (x_2) in case that $x_1 = x_2$ for all inputs x_1,and x_2.

As G → $n \times n$ S-Box

2.1 Practical examples for S-Box Test Criteria

This section includes some tests for S-boxes shown in Figure (1) were generated using a proposed method to generate a key dependent-S-Boxes, where a keys were used to generate these S-Boxes, the results of the tests Criteria will be shown in the next figures.

0Xfe	0X76	0Xf2	0X6f	0X01	0Xc5	0X7b	0X6b	0X67	0Xab	0X2b	0X77	0Xd7	0X63	0X7c	0X30
0X47	0Xc0	0Xca	0Xa4	0X9c	0Xf0	0Xaf	0X72	0Xd4	0X59	0Xa2	0Xfa	0X7d	0Xad	0Xc9	0X82
0Xa5	0X31	0Xd8	0Xf7	0Xfd	0X34	0Xb7	0X26	0X36	0X15	0X71	0Xe5	0X93	0Xcc	0Xf1	0X3f
0Xb2	0X75	0X27	0Xc7	0Xe2	0X80	0X07	0X04	0X9a	0Xeb	0Xc3	0X05	0X96	0X18	0X23	0X12
0X1a	0X52	0X2f	0Xe3	0Xd6	0X6e	0Xb3	0X5a	0X84	0X83	0X29	0X3b	0Xa0	0X09	0X1b	0X2c
0X4a	0Xbe	0Xd1	0Xb1	0X39	0X6a	0X4c	0Xcb	0X5b	0Xcf	0X58	0X20	0Xed	0X0	0Xfc	0X53
0Xa8	0Xef	0X4d	0Xf9	0X43	0X3c	0X7f	0Xd0	0X02	0Xfb	0X33	0Xaa	0X45	0X85	0X50	0X9f
0Xda	0Xd2	0Xb6	0Xa3	0X51	0Xff	0Xbc	0X21	0X10	0X40	0X8f	0X9d	0Xf3	0Xf5	0X38	0X92
0X44	0X5f	0Xc4	0X64	0X3d	0X13	0X7e	0X73	0X5d	0X19	0Xcd	0X0c	0X17	0Xec	0X97	0Xa7
0X14	0X46	0X2a	0Xb8	0X0b	0X5e	0X4f	0X88	0X60	0X81	0X22	0X90	0Xdc	0Xde	0Xee	0Xdb
0X95	0Xc2	0X0a	0X62	0X49	0Xd3	0X24	0X79	0X06	0X5c	0Xac	0X3a	0X32	0Xe4	0X91	0Xe0
0X08	0Xd5	0Xae	0X6d	0X65	0Xea	0X37	0X8d	0Xf4	0Xc8	0X7a	0Xa9	0X6c	0X56	0X4e	0Xe7
0X25	0X74	0X78	0Xa6	0X2e	0X4b	0Xbd	0Xdd	0Xe8	0X1f	0X8b	0Xb4	0Xba	0Xc6	0X8a	0X1c
0Xb9	0X0e	0Xb5	0X61	0X86	0Xc1	0X03	0X48	0X57	0X3e	0X35	0X9e	0Xf6	0X70	0X1d	0X66
0X87	0Xdf	0X55	0X9b	0Xd9	0X98	0X69	0X28	0Xf8	0X11	0X94	0X1e	0X8e	0Xe9	0Xce	0Xe1
0X68	0X0f	0Xa1	0Xbb	0X2d	0X54	0X16	0Xbf	0X8c	0X99	0X0d	0Xb0	0X89	0X42	0X41	0Xe6

0X30	0Xab	0Xd7	0X77	0Xc5	0Xfe	0X63	0X7b	0X6f	0X6b	0X01	0X7c	0Xf2	0X2b	0X76	0X67
0X59	0X7d	0Xaf	0X72	0Xca	0Xfa	0X9c	0Xd4	0X82	0X47	0Xc9	0Xa4	0Xad	0Xf0	0Xc0	0Xa2
0X31	0X34	0Xf7	0X3f	0Xf1	0Xa5	0Xe5	0X93	0Xcc	0X26	0Xb7	0Xd8	0Xfd	0X71	0X36	0X15
0Xc3	0X12	0X18	0X04	0Xeb	0X05	0X96	0X9a	0Xb2	0Xc7	0X27	0X75	0X07	0Xe2	0X23	0X80
0X6e	0X9	0X29	0X1a	0X5a	0Xe3	0X2c	0X84	0Xb3	0X1b	0X3b	0X2f	0Xd6	0X52	0Xa0	0X83
0X5b	0Xcf	0X20	0X4a	0X53	0X00	0Xbe	0X6a	0Xfc	0Xd1	0X58	0Xed	0X4c	0Xcb	0Xb1	0X39
0Xa8	0X2	0Xaa	0X7f	0X50	0X85	0X45	0Xd0	0Xef	0X9f	0X4d	0Xf9	0X33	0Xfb	0X43	0X3c
0X40	0Xda	0X21	0Xf5	0X8f	0Xd2	0X92	0Xa3	0X51	0X10	0X38	0Xf3	0X9d	0Xbc	0Xff	0Xb6
0Xcd	0X19	0Xa7	0X64	0Xc4	0X17	0X44	0X7e	0X3d	0X5d	0X97	0X73	0Xec	0X13	0X5f	0X0c
0X88	0Xdb	0Xb8	0X46	0X2a	0X5e	0X81	0X22	0X14	0X0b	0X60	0Xde	0X90	0X4f	0Xee	0Xdc
0X0a	0Xe4	0X3a	0Xac	0X79	0X49	0Xe0	0X24	0Xd3	0X5c	0Xc2	0X06	0X32	0X91	0X62	0X95
0Xd5	0X6c	0Xe7	0X37	0Xf4	0Xae	0Xea	0X08	0X8d	0X65	0X56	0X7a	0X4e	0X6d	0Xa9	0Xc8
0X8a	0Xdd	0Xe8	0X4b	0X1f	0Xa6	0Xbd	0X2e	0X1c	0Xba	0X78	0X8b	0Xb4	0X74	0Xc6	0X25
0X66	0X3	0Xb9	0X3e	0X35	0X48	0Xc1	0Xf6	0X1d	0X61	0X0e	0X57	0X86	0Xb5	0X9e	0X70
0X87	0Xe1	0X9b	0X69	0X94	0Xdf	0X11	0X8e	0Xce	0X1e	0X55	0X98	0X28	0Xd9	0Xe9	0Xf8
0X0d	0X54	0X99	0Xbf	0Xe6	0X89	0X0f	0X2d	0X8c	0Xa1	0X68	0X41	0X16	0Xbb	0Xb0	0X42

0xa0	0x7d	0x52	0x2d	0x5c	0x26	0x35	0x0b	0xfd	0x9c	0x2e	0x2b	0x47	0x5e	0x84	0x0d
0xc9	0xc3	0x3c	0x69	0x3b	0xb5	0xa6	0x08	0x83	0xbb	0xba	0xa8	0x49	0x82	0x4d	0x96
0x00	0x5a	0xb2	0x60	0x1c	0xa2	0xb1	0xcb	0xbd	0xdc	0xa7	0xaf	0x80	0xbc	0x44	0x05
0x09	0x1f	0xa5	0x55	0xcc	0xf5	0xe6	0x02	0xd3	0x7b	0x3e	0xec	0x89	0xd2	0x30	0xd6
0xc0	0x9a	0xf6	0x10	0xcf	0x62	0x11	0x7c	0x0a	0x2c	0x23	0xef	0x40	0x01	0x5d	0xc5
0x4a	0xae	0xe5	0x95	0xd8	0x45	0x9e	0xc2	0x50	0x6f	0x7e	0xbf	0xca	0x12	0xf0	0xe2
0xdf	0xf7	0xb6	0xd0	0x7f	0x56	0xd1	0x51	0x15	0x6c	0xe3	0x98	0x13	0xc1	0xad	0x75
0xea	0xee	0x85	0x39	0x18	0xc4	0x42	0x1e	0x90	0x2f	0xce	0xff	0x43	0x4b	0xe4	0x71
0xf3	0xb7	0x16	0x07	0xab	0xd9	0xfc	0x91	0xd5	0x28	0xd7	0x58	0xda	0x88	0xed	0x36
0x2a	0xfa	0x8d	0x79	0x68	0x74	0x46	0xde	0xe0	0x94	0x0e	0x4f	0x9f	0x8b	0xa4	0x65
0xb3	0x67	0x04	0xc7	0x6b	0x19	0xf8	0xe1	0x1d	0xdb	0x97	0x4c	0x1a	0x48	0xa9	0x76
0xfe	0x3a	0xcd	0x93	0x54	0x34	0x86	0xf2	0xb4	0x38	0xe7	0x8f	0x5f	0x14	0x20	0x25
0x63	0x27	0x64	0x8a	0x1b	0x9d	0xb8	0x21	0x99	0x06	0x7a	0x0c	0x6a	0x9b	0xe9	0x32
0x4e	0xbe	0x6d	0x53	0x41	0xb0	0x5b	0xf1	0xf4	0x78	0x37	0x8c	0x73	0xd4	0xb9	0xa1
0x57	0xa3	0x24	0x3d	0x92	0xdd	0xac	0x66	0x59	0xc6	0x6e	0x0f	0xaa	0xeb	0x87	0x72
0x8e	0x17	0x29	0x03	0x81	0x70	0xfb	0x31	0x22	0xc8	0x77	0x3f	0x33	0xe8	0xf9	0x61

Figure 1: An examples of the produces key-dependent S-Boxes

2.1.1 Balanced

The experimental outcomes illustrate that whole resulted S-Boxes have the equal amounts of zeroes and ones, representing that the S-Boxes are balanced.

2.1.2 Completeness

For generated S-Boxes, the experimental results illustrated that this S-Box fulfils the completeness feature because every bit of the produced S-Boxes is subjected to the whole of the input bits.

2.1.3 Avalanche criterion

According to Equation 7, the avalanche criterion was evaluated for produced S-Boxes, the experiment outcomes illustrated that the S-Boxes' avalanche values are within 0.46, and 0.49. This indicates all the generated S-Boxes satisfy the avalanche effect with a value close to the ideal value since the ideal avalanche value is equal to 0.5. as shown in Figure 2.

S-Box Sequence	*Avalanche*
1	0.48046875421
2	0.47705078125
3	0.48486328128
4	0.46972665625
5	0.48846843755
6	0.49021456426
7	0.469447265625
8	0.47362815855

Figure 2: An Example of Avalanche values of the produced S-boxes

2.1.4 Strict avalanche (SAC)

The experimental results showed that the SAC values range between 122 and 132. This indicates that all these generated S-Boxes satisfy the SAC with a value close to the ideal value of 128, where the probabilistic approach is 0.5, for n = 8, as whenever a single bit of inputs is inverted, its corresponding output bit will inverse with the probability of approaching 0.5 (Cui, et al. 2011).

2.1.5 Nonlinearity

According to Equation 12, the nonlinearity criterion, NL(S) for the key-dependent S-Boxes (rounds S-Boxes).

The experimental results showed that the nonlinearity values for all generated S-Box, are not less 108, with all positive values. This indicates that most of these S-Boxes are very close to NL(S) of the perfect nonlinear function, proving that they have good resistance against linear cryptanalysis (Cui, et al. 2011).

This indicates that these S-Boxes have respectable nonlinearity because the perfect nonlinearity amount for *n* is equal to 8 (*n* represents the number of input bits) is 120, as (Wen, et al. 2000) mentioned that the NL(S) of perfect nonlinear function should be NL(S) = $2^{n-1} - 2^{\frac{n}{2}-1}$ = 120 (for n = 8), The S-Boxes are not a perfect nonlinearity function, but NL is very close to the NL(S) of perfect nonlinear function, and provided the amount of nonlinearity is greater than 100, this indicates it has respectable resistance against the linear cryptanalysis since the resistance against linear cryptanalysis is measured by Nonlinearity (Hussain, et al. 2011; Kazymyrov, et al.).

2.1.6 Bit independence (BIC)

According to Equation 15, the bit independence criterion was evaluated for the S-Boxes. For the produced S-Boxes, the experimental results showed that the BIC values range between 0.025, and 0.078125. This indicates that produced S-Boxes are secure enough since they have BIC values far from 1, (the worst state for BIC), and close to 0, (the ideal state for BIC) (Webster and Tavares 1986).

2.1.7 Differential uniformity

According to Equation 17, the Differential Uniformity criterion was evaluated for the key-dependent S-Boxes, the results illustrated that the $\delta(G)$ values are not more than 10.

It's known that AES S-Box has δ(G) lower of 10, as well as the impedance against differential cryptanalytics can be evaluated by δ(G). The results indicates the safety of the formed S-Boxes (Mamadolimov, et al. 2013), resistance against the differential cryptanalysis as reading the tiny value of δ(G) shows its stands against differential attack (Cui, et al. 2011) (Tan, et al. 2015).

2.1.8 Invertability

The results of the produced S-Boxes showed that all of them fulfilled this criterion.

2.1.9 Non-contradiction

The experimental results showed that all the proposed S-Boxes that key-dependent S-Boxes have the non-contradiction criterion, as all the tested S-Boxes had only one non repeated value in every cell of the table.

3.0 Conclusion

This article provides information can be used as a guide for the researchers that concern with the designing and implementation of block ciphers especially the substitution unit (S-Box). The use of these criteria is essential in evaluating the designing any encryption algorithm.

4.0 References

Adams, Carlisle, and Stafford Tavares
1990 Good S-boxes are easy to find. Advances in Cryptology—CRYPTO'89 Proceedings, 1990, pp. 612-615. Springer.

Bogdanov, Andrey, et al.
2012 Key-Alternating ciphers in a provable setting: encryption using a small number of public permutations. *In* Advances in Cryptology–EUROCRYPT 2012. Pp. 45-62: Springer.

Braeken, Ann
2006 Cryptographic properties of Boolean functions and S-boxes, phd thesis-2006.

Canteaut, Anne, and Marion Videau
2005 Symmetric boolean functions. Information Theory, IEEE Transactions on 51(8):2791-2811.

Carlet, Claude, and Cunsheng Ding
2007 Nonlinearities of S-boxes. Finite Fields and Their Applications 13(1):121-135.

Coskun, Baris, and Nasir Memon
2006 Confusion/diffusion capabilities of some robust hash functions. Information Sciences and Systems, 2006 40th Annual Conference on, 2006, pp. 1188-1193. IEEE.

Cui, Jie, et al.
2011 An improved AES S-Box and its performance analysis. International Journal of Innovative Computing, Information and Control 7(5).

Cui, Lingguo, and Yuanda Cao
2007 A new S-box structure named Affine-Power-Affine. International Journal of Innovative Computing, Information and Control 3(3):751-759.

Daemen, Joan, and Vincent Rijmen
2002 The design of Rijndael: AES-the advanced encryption standard: Springer.

Feistel, Horst
1973 Cryptography and computer privacy. Scientific american 228:15-23.

Feistel, Horst, William A Notz, and J Lynn Smith
1975 Some cryptographic techniques for machine-to-machine data communications. Proceedings of the IEEE 63(11):1545-1554.

Gao, Sheng, Wenping Ma, and Jiwei Zhu

2012 Nonlinearity Profile Test for an S-Box. *In* Future Wireless Networks and Information Systems. Pp. 639-644: Springer.

Gong, Guang, Yin Tan, and Bo Zhu

Enhanced Criteria on Differential Uniformity and Nonlinearity of Cryptographically Significant Functions.

Hussain, Iqtadar, et al.

2011 Construction of cryptographically strong 8× 8 S-boxes. World Appl. Sci. J 13(11):2389-2395.

Kazlauskas, Kazys, and Jaunius Kazlauskas

2009 Key-dependent S-box generation in AES block cipher system. Informatica 20(1):23-34.

Kazymyrov, Oleksandr, Valentyna Kazymyrova, and Roman Oliynykov

A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent.

Knudsen, Lars R, and Matthew Robshaw

2011 The Block Cipher Companion. Information security and cryptography. Springer 6:17-35.

Lai, Xuejia

1992 On the design and security of block ciphers, Diss. Techn. Wiss ETH Zürich, Nr. 9752, 1992. Ref.: JL Massey; Korref.: H. Bühlmann.

law Szaban, Miros, and Franciszek Seredynski

CA-based S-boxes for Secure Ciphers.

Mamadolimov, Abdurashid , Herman Isa, and Moesfa Soeheila Mohamad

2013 Practical bijective S-box design. arXiv preprint arXiv:1301.4723.

Meier, Willi, and Othmar Staffelbach

1990 Nonlinearity criteria for cryptographic functions. Advances in Cryptology—EUROCRYPT'89, 1990, pp. 549-562. Springer.

Pieprzyk, J, and G Finkelstein

1988 Towards effective nonlinear cryptosystem design. Computers and Digital Techniques, IEE Proceedings E 135(6):325-335.

Ramanujam, Sriram, and Marimuthu Karuppiah

2011 Designing an algorithm with high avalanche effect. IJCSNS 11(1):106.

Shannon, Claude E

1949a Communication theory of secrecy systems. Bell system technical journal 28(4):656-715.

—

1949b Communication Theory of Secrecy Systems*. Bell system technical journal 28(4):656-715.

Standard, Data Encryption
1977 FIPS PUB 46. Appendix A, Federal Information Processing Standards Publication.

Tan, Yin, GUANG GONG, and Bo Zhu
2015 Enhanced criteria on differential uniformity and nonlinearity of cryptographically significant functions.

Vergili, Isıl, and MD Yücel
2001 Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen× S-Boxes. Turk J Elec Engin 9(2):137-145.

Webster, AF, and Stafford E Tavares
1986 On the design of S-boxes. Advances in Cryptology—CRYPTO'85 Proceedings, 1986, pp. 523-534. Springer.

Wen, Q-y, Xinxin Niu, and Yixian Yang
2000 The Boolean Functions in modern cryptology: Beijing: Science Press.

William, Stallings, and William Stallings
2006 Cryptography and Network Security, 4/E: Pearson Education India.