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

Dr. Auday H. Saeed AL-Wattar*
Ahsa.alwattar@uomensul.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

This is an open access article under the CC BY 4.0 license http://creativecommons.org/licenses/by/4.0/

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

This is an open access article under the CC BY 4.0 license http://creativecommons.org/licenses/by/4.0/

استعراض معايير فحص صناديق الاستبدال للتشغيل المقطعي

المستخلص

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

استخدام وظائف الاستبدال والتشكيل بشكل شائع في خوارزميات التشغيل المقطعي لجعلها أكثر صعوبة وفعالية. ان امنية صندوق الاستبدال يتم فحصها أو 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 بالتشغيل المقطعي حيث تتضمن هذه الورقة مسما أو دليل لمعايير اختيار 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.

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

$$p = E_k^{-1}(C)$$  \hspace{1cm} (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:

$$E : F_2^n \times F_2^k \rightarrow F_2^n$$

These are equivalent to:

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

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 \( n \times m \) 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\} : \ \forall \ 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\}

\[ W = [w_{n-1}, w_{n-2}, \ldots, w_1, w_0], \text{ where } w_{n-1}, w_{n-2}, \ldots, w_1, w_0 \in \{0,1\}. \]

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

\[ \sum_{W \in \{0,1\}^n} f(W) = 2^{n-1} \tag{4} \]

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

\[ \forall 0 \leq j \leq n - 1, \ \ \exists \in \{0,1\}^n \ \sum_{W \in \{0,1\}^n} f_i(X) \oplus f_i(X \oplus \alpha) = 2^{n-1} \tag{5} \]

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 zi ) and, Y(z) and Y(z_i) differ leastwise in bit h, for whole \{i, h : 1 \leq i, h \leq 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 \( n \times n \) square s-box \( S: \{0,1\}^n \rightarrow \{0,1\}^n \) is consider complete, if for all vectors, 
\( A = [a_{n-1}, ..., a_1, a_0] \in \{0,1\}^n \) which hamming wight is 1, \( hw(A) = 1 \), there exists vector \( W = [w_{n-1}, w_{n-2}, ..., w_1, w_0] \in \{0,1\}^n \), such that \( S(W) \) and \( S(W \oplus A) \) are dissimilar on bit \( i \) for all \( i \in \{n-1, ..., 1, 0\} \).

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:

\[
hw(W) = \sum_{i=0}^{n-1} w_i
\]  

\[6\]

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.

\[
AV_{C_u} = Y(y) \oplus Y(y \oplus c_i) = av_1^{C_u} av_2^{C_u} av_3^{C_u} ... av_m^{C_u}
\]

\[7\]

Properly, the criterion of avalanche can be exemplified as:

\( S: \{0,1\}^m \rightarrow \{0,1\}^m \)

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 \( u \in (1,...,2^m) \): where S is a square S-Box with \( m \times m \).

\[
\frac{1}{2^m} \sum_{v=1}^{m} W(\av_{v}^{C_u}) = \frac{m}{2}
\]

\[8\]

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

\[
W(\av_{v}^{C_u}) = \sum_{x \in \{0,1\}^n} (\av_{x}^{C_u})
\]

\[9\]

\( Avalanche \text{ Effect} = \frac{1}{m2^m} \sum_{v=1}^{m} W(\av_{v}^{C_u}) = 0.5 \)

\[10\]
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 \{-\in A, +\in 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 Karuppijah 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, ..., 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

\[
Strict\; Avalanche\; Effect = \frac{1}{2^t} W(\text{av}_e^c) = 0.5 \quad (11)
\]

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: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m \quad \text{As } F: \{0,1\}^n \rightarrow \{0,1\}

And G (d) is a Boolean function such as G (d) \in BFn over \mathbb{F}_2^n

\[
w_G(d) = \sum_{d \in \mathbb{F}_2^n} (-1)^{f(d) \oplus [d,v]}
\]

Where \; w_G is Walsh transformation of G(d)

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

\[
NL(G) = 2^{n-1} - \frac{1}{2} \max_{d \in \mathbb{F}_2^n} |W_G(d)| \quad (13)
\]
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 $2^{t-1} - 2^{z-1}$ 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.

$$\text{NL}(G) = \min_{z \in \mathbb{F}_2^n} \max_{x \in \{0\}} \text{NL}([z, F])$$  \hspace{1cm} (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,..., t), as y ≠ l, fulfills 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 $AV^{c,d}$

$$BIC(a_e, a_y) = \max_{1 \leq d \leq t} \left| Corr(a_v^{ed}, a_y^{ed}) \right|$$  \hspace{1cm} (15)

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

$$BIC(S) = \max_{1 \leq v,y \leq t} BIC(ad, ay)$$  \hspace{1cm} (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

$$\delta(G) = \max_{\alpha \in F_2^n} \left| \{x | G(x) + G(x + \alpha) = \beta \} \right|$$  \hspace{1cm} (17)

As: $G(x) = (g(x), ..., g_n(x))$, is a multiple product Boolean function of $F_2^n \rightarrow F_2^n$. 
The lowest value for $\delta(G) = 1$, the small amount of $\delta(G)$ indicates it has a good reluctant against differential attack (Gong, et al.).

**H. Invertability**

The S-Box fulfils the invertability states, if:

$$G(x_1) = G(x_2) \text{ in case that } x_1 = x_2 \text{ for all inputs } x_1 \text{ and } x_2.$$

As $G \rightarrow n \times n$ 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.

#### 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

![Figure 1: An examples of the produces key-dependent S-Boxes](image-url)
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.

![Figure 2: An Example of Avalanche values of the produced S-boxes](image)

### 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^{n-1} = 120 (for n = 8), The S-Boxes are not a perfect nonlinear 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 \(\delta(G)\) lower of 10, as well as the impedance against differential cryptanalytics can be evaluated by \(\delta(G)\). 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 \(\delta(G)\) 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 Soheila 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.