Turk J Elec Engin, VOL.9, NO.2 2001, © TÜBİTAK

Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen $n \times n$ S-Boxes

Işıl VERGİLİ, Melek D. YÜCEL
EE Department of METU, TÜBİTAK-BİLTEN, Ankara-TURKEY

Abstract

Cryptographic test methods such as avalanche, strict avalanche and bit independence criteria, which measure the degree of security of the s-boxes of substitution-permutation networks, are applied to randomly generated ensembles of $n \times n$ s-boxes. Statistical analysis of experimental data directs the work towards defining "relative errors" and examining the avalanche and strict avalanche criteria within "relative error ranges". Histograms of relative errors in each ensemble are evaluated, and combining the results of different ensembles corresponding to different values of the s-box size, variations of maximum relative errors versus the size of the s-box are depicted. Some predictions follow that the larger the s-box size, the more probable that these criteria are satisfied; thus it is possible to form more secure substitution-permutation networks. Correlations among the test criteria are also evaluated in random ensembles to find out to what extent those criteria measure different cryptographic aspects of s-boxes.

1. Introduction

Substitution Permutation Networks (SPNs) are a simple yet elegant class of secret key ciphers having *substitution boxes* (s-boxes) as critical components. An SPN consists of rounds of substitutions (s-boxes) followed by bit permutations, and these two stages convert plaintexts into encrypted ciphertexts. Substitution stage maps input vectors nonlinearly into output vectors, and permutation stage "diffuses", that is, mixes up the plaintext further. These two stages can be applied to the plaintext one after the other in a predefined number of rounds, in order to increase security.

Briefly, an $n \times n$ s-box is a mapping function, $\boldsymbol{f}$: $\{0,1\}^n \rightarrow \{0,1\}^n$, which maps n-bit input strings, $\mathbf{X}$, to $n-$ bit output strings, $\mathbf{Y}$, where $\mathbf{Y} = \boldsymbol{f}(\mathbf{X})$. Much of the research about s-boxes has focused on determining s-box properties, which yield a cryptographically strong SPN. To have a secure SPN, s-boxes should satisfy some dynamic properties such as avalanche, strict avalanche and bit independence, which deal with the relationships between plaintext and ciphertext changes.

As these properties are based on the bit changes in the input/output bit strings of the s-box, we need to define the following terms used in determining these relations:

$\boldsymbol{e}_i$ is the unit vector with bit i equal to 1 and all other bits equal to 0.

$\boldsymbol{A}^{ei}$ is the output difference string, called the avalanche vector, when only the i'th bit in the input string is changed. It is defined as:

$$A^{ei} = f(\mathbf{X}) \oplus f(\mathbf{X} \oplus e_i) = [a_1^{ei} a_2^{ei} \ldots a_n^{ei}], \tag{1}$$

where $a_j^{ei} \in \{0,1\}$.

The properties mentioned above are regarded as a measure of how randomly the ciphertext changes when the plaintext bits are changed, and they are explained in detail in Section 2. Interpretation of the avalanche and strict avalanche criteria within relative error regions is proposed in Section 3 and is supported by experimental results. Section 4 is a discussion on the correlations among mentioned criteria, to find out whether they measure different cryptographic aspects of a given s-box.

2. Criteria and Definitions

2.1. Avalanche Criterion

Feistel et al. defined a property of s-boxes and SPN's known as *Avalanche (AVAL) Criterion* [1, 2]. The *AVAL* criterion is an important cryptographic property of block ciphers which says that a small number of bit differences in the input plaintext leads to an "avalanche" of changes, that is, results in a large number of ciphertext bit differences. More formally, a function $\boldsymbol{f}: \{0,1\}^n \rightarrow \{0,1\}^n$ satisfies the *AVAL* criterion if whenever one input bit is changed, on the average, half of the output bits change, where i and $j \in (1,2,\ldots,n)$ are input and output bits respectively. Formulating this, an $n \times n$ s-box is said to satisfy the *AVAL* criterion if for all $i = 1,2,\ldots,n$:

$$\frac{1}{2^n}\sum_{j=1}^{n} W(a_j^{e_i}) = \frac{n}{2} \tag{2}$$

where

$$W(a_j^{e_i}) = \sum_{allX \in \{0,1\}^n} a_j^{e_i} \tag{3}$$

is the total change in the j'th avalanche variable, a_j^{ei}, computed over the whole input alphabet of size 2^n (Note that $0 \leq W(a_j^{ei}) \leq 2^n$).

We can manipulate (2) to define an *AVAL* parameter, $k_{AVAL}(i)$ as

$$k_{AVAL}(i) = \frac{1}{n2^n}\sum_{j=1}^{n} W(a_j^{e_i}) = \frac{1}{2} \tag{4}$$

$k_{AVAL}(i)$ can take values in the range [0,1], and it should be interpreted as the probability of change of the overall output bits when only the i'th bit in the input string is changed. If $k_{AVAL}(i)$ is different from $1/2$ for any i, then it is conjectured that the s-box does not satisfy the *AVAL* criterion. However, our experimental results given in Section 3 show that exact satisfaction of (4) for all values of i is not a realistic expectation, and it is much wiser to interpret (4) within an error interval of $\{-\in_A, +\in_A\}$ which is defined and discussed in Section 3.1.

2.2. Strict Avalanche Criterion (SAC)

In 1985, Webster and Tavares combined the completeness and avalanche properties into the *Strict Avalanche Criterion* (*SAC*) [3]. A function $\boldsymbol{f}$: $\{0,1\}^n \rightarrow \{0,1\}^n$ satisfies the *SAC* if for all $i,j \in (1,2,\ldots,n)$, flipping

input bit i changes the output bit j with the probability of exactly one half. So an s-box satisfies the *SAC* if

$$\frac{1}{2^n} W(a_j^{e_i}) = \frac{1}{2} \quad \text{, for all } \; i, j. \tag{5}$$

(5) can be modified in order to define a *SAC* parameter, $k_{SAC}(i, j)$ as

$$k_{SAC}(i, j) = \frac{1}{2^n} W(a_j^{e_i}) = \frac{1}{2} \tag{6}$$

$k_{SAC}(i, j)$ can take values in the range [0,1], and it should be interpreted as the probability of change of the j'th output bit when the i'th bit in the input string is changed. If $k_{SAC}(i, j)$ is different from $1/2$ for any (i, j) pair, then the s-box is said not to satisfy the *SAC*. However, our experimental results given in Section 3 show that exact satisfaction of (6) for all values of i and j is not a realistic expectation, and it is much more meaningful to interpret (6) within an error interval of $\{-\in_S, +\in_S\}$, which is defined and discussed in Section 3.2.

It is apparent that the *AVAL* criterion and *SAC* are very similar and it is easy to demonstrate that an s-box, that satisfies the *SAC* must also satisfy the *AVAL* criterion, but the satisfaction of the *AVAL* criterion does not necessarily imply the satisfaction of the *SAC*.

2.3. Bit Independence Criterion (BIC)

Webster and Tavares defined another property called the *Bit Independence Criterion* (*BIC*) for s-boxes [3]. A function $\boldsymbol{f} : \{0,1\}^n \to \{0,1\}^n$ satisfies the *BIC* if for all $i, j, k \in \{1, 2, \ldots, n\}$, with $j \neq k$, inverting input bit i causes output bits j and k to change independently.

To measure the bit independence concept, one needs the *correlation coefficient* between the j'th and k'th components of the output difference string, which is called the avalanche vector $\boldsymbol{A}^{ei}$. A bit independence parameter corresponding to the effect of the i'th input bit change on the j'th and k'th bits of $\boldsymbol{A}^{ei}$ is defined as

$$BIC(a_j, a_k) = \max_{1 \leq i \leq n} |corr(a_j^{e_i}, a_k^{e_{i'}})| \tag{7}$$

Overall, the Bit Independence Criterion (*BIC*) parameter for the s-box function $\boldsymbol{f}$ is then found as

$$BIC(f) = \max_{\substack{1 \leq j, k \leq n \\ j \neq k}} BIC(a_j, a_k) \tag{8}$$

which demonstrates how close $\boldsymbol{f}$ is to satisfying the *BIC* [4]. *BIC*($\boldsymbol{f}$) takes values in [0, 1]. It is ideally equal to 0 and, in the worst case, it is equal to1.

3. Definition of Relative Errors and Experimental Results

In order to investigate the statistics of the s-box properties mentioned in the previous section, some experiments are performed over ensembles of $n \times n$ s-boxes. For different values of $n \leq 16$, different ensembles of 10,000 randomly chosen $n \times n$ s-boxes are formed. Considering the input string $\mathbf{X}$ and output string $\boldsymbol{f}(\mathbf{X})$

as binary representations of the integers, $l \in \{0, 1, 2, ..., 2^n - 1\}$, each s-box is generated by mapping the input $l = 0, 1, 2, ..., 2^n - 1$ to a randomly chosen output from the set of integers $\{0, 1, 2, ..., 2^n - 1\}$ with equal probabilities. Also note that these s-boxes are generated with the constraint that their defining functions, $\boldsymbol{f}(\mathbf{X})$, are one to one, and $\boldsymbol{f}(\mathbf{X}) \neq \mathbf{X}$.

3.1. Relative Error for the Avalanche Criterion

Statistical analysis of the experimental data over many ensembles of $n \times n$ s-boxes shows that it is possible to find s-boxes satisfying (4) for small values of n, but for n=6 and larger, it becomes very difficult to satisfy the *AVAL* criterion exactly. Therefore, it seems more logical to expect the criterion given by (4) to be satisfied within an error range of $\pm \in_A$, which is called the *relative error interval for the AVAL criterion.* We say that an s-box satisfies the *AVAL* criterion within $\pm \in_A$ if for all i

$$\frac{1}{2}(1- \in_A) \leq k_{AVAL}(i) \leq \frac{1}{2}(1+ \in_A) \tag{9}$$

is true. Given an s-box, the corresponding relative error $\in_A$ can be found from (9) as

$$\in_A = \max_{1 \leq i \leq n} |2k_{AVAL}(i) - 1| \tag{10}$$

Each of the 10,000 random s-boxes of an ensemble has a specific relative error value $\in_A$. That is, it satisfies the *AVAL* criterion within $\pm \in_A$. The distribution of $\in_A$ values in an ensemble can be shown by a histogram which indicates the number of occurrences of each $\in_A$ value in the ensemble. Sample histograms are given in Figure 1 for an ensemble of 10 $\times$ 10 s-boxes. Figure 1 gives a clear idea as to relative error statistics of the *AVAL* for randomly chosen s-boxes. Almost all s-boxes of the ensemble seem to satisfy the *AVAL* criterion within $\pm 7\%$, and the majority is clustered around a relative error value of ± 2 or $\pm 3\%$.

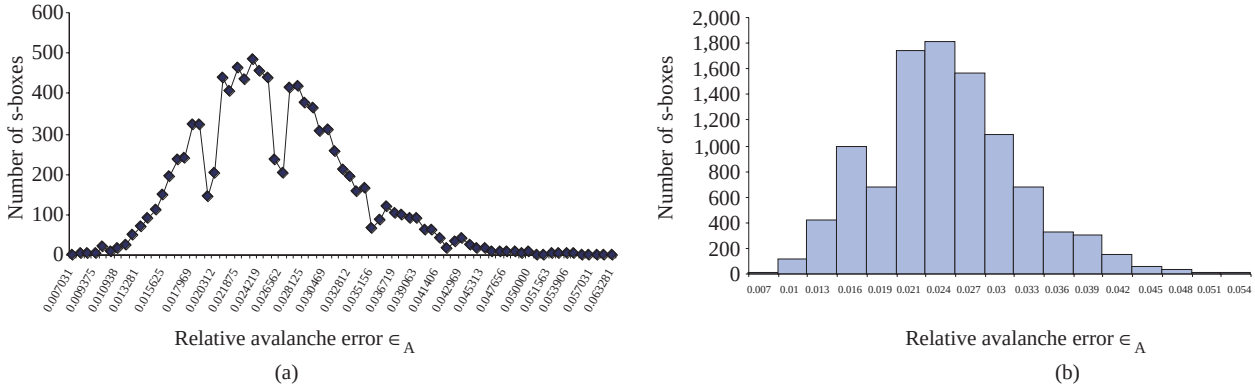


Figure 1. Histograms for relative error values $\in_A$ of the *AVAL* criterion for an ensemble of 10×10 s-boxes (a) with fine intervals (b) with coarse intervals

The maximum of all $\in_A$ values determines the upper limit of relative error to satisfy the *AVAL* criterion, for the $n \times n$ s-boxes of the ensemble. Then, after calculating all $\in_A$'s using (10), we find the maximum of all, and name this *maximum relative error for the AVAL criterion* as $\in_{AVAL}$

$$\in_{AVAL} = \max_{over\ all\ s-boxes} \{\in_A\} \tag{11}$$

To show the relation between $\in_{AVAL}$ values and s-box size n, experiments are performed for different ensembles of $n \times n$ s-boxes. Figure 2 shows that $\in_{AVAL}$ decreases exponentially as n is increased, and for large s-boxes of size 16x16, all the relative error values in the ensemble fall below 1% , with $\in_{AVAL} = 0.47\%$.

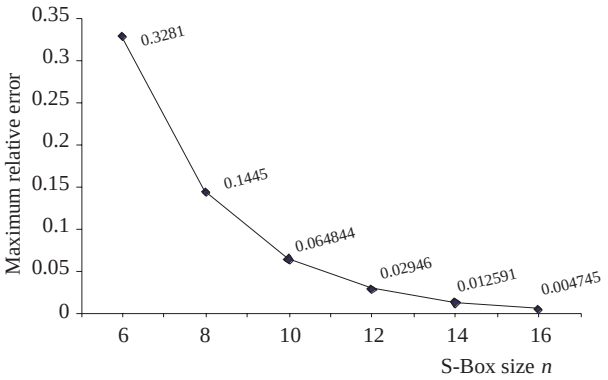


Figure 2. Maximum relative error $\in_{AVAL}$ versus s-box size n

3.2. Relative Error for the Strict Avalanche Criterion

SAC is a more specialized form of the $AVAL$ criterion, so the number of s-boxes satisfying SAC is smaller than the number of s-boxes satisfying the $AVAL$ criterion, as expected. Again, for $n = 6$ and larger, s-boxes that satisfy the SAC within a relative error interval may be found. Therefore modifying (6), an s-box satisfies the SAC within $\pm \in_S$ if for all i and j, the following equation is satisfied:

$$\frac{1}{2}(1- \in_S) \leq k_{SAC}(i,j) \leq \frac{1}{2}(1+ \in_S) \tag{12}$$

Using (12) for a given s-box, relative error the $\in_S$ for SAC can be found as

$$\in_S = \max_{1 \leq i,j \leq n} |2k_{SAC}(i,j) - 1| \tag{13}$$

Each of the 10,000 random s-boxes of an ensemble has a specific relative error value $\in_S$. That is, it satisfies the SAC within $\pm \in_S$. For the ensembles of randomly generated $n \times n$ s-boxes, we calculate $\in_S$ values corresponding to each s-box and sketch their distribution as histograms. Figure 3 is an example histogram for $n = 10$, and gives a clear idea on relative error statistics of the SAC for randomly chosen s-boxes. Almost all the s-boxes of the ensemble seem to satisfy the SAC within $\pm$21-22% , and the majority is clustered around a relative error value of $\pm$10-11% .

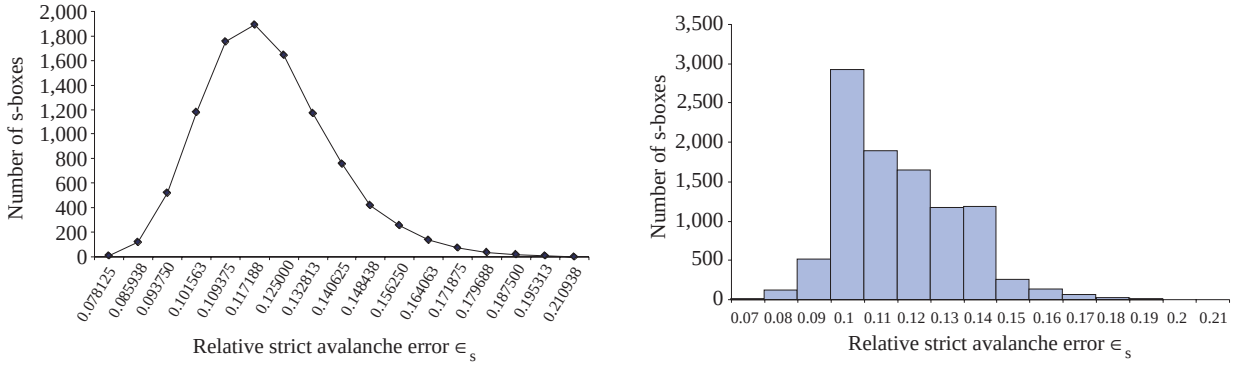


Figure 3. Histograms for relative error values $\in_S$ of SAC for an ensemble of 10 $\times$ 10 s-boxes (a) with fine intervals (b) with coarse intervals

After calculating all relative errors using Eq. (16), we find the largest $\in_S$ value among all s-boxes in the ensemble and denote this *maximum relative error for SAC* by $\in_{SAC}$

$$\in_{SAC} = \max_{over\ all\ s-boxes} \{\in_S\} \tag{14}$$

Figure 4 shows the variation of $\in_{SAC}$ values versus different values of the s-box size n, which we obtain experimentally [5, 6] by considering different ensembles of size $n \times n$.

Similarly to the behaviour of maximum relative avalanche error $\in_{AVAL}$, maximum relative SAC error $\in_{SAC}$ also decreases exponentially with increasing n. It is observed from Figure 4 that, for large s-box sizes, the probability that randomly created s-boxes satisfy the SAC with small relative errors is quite high. For s-boxes of size 16x16, all the relative error values in the ensemble fall below $\in_{SAC} = 2.31\%$.

3.3. Bit Independence Criterion

The situation for the BIC is a little different from the $AVAL$ criterion and the SAC, as the BIC is analysed according to the $BIC(\boldsymbol{f})$ value of an s-box, which is already defined by (11) as the highest correlation between any two bits, hence relative error $\in_B$ is equal to $BIC(\boldsymbol{f})$ for this criterion. Then, for a set of $n \times n$ s-boxes, the largest of $\in_B = BIC\ (\boldsymbol{f})$ values obtained by (11) is found and named the *maximum relative error for the BIC*, and denoted by $\in_{BIC}$

$$\in_{BIC} = \max_{over\ all\ s-boxes} \{\in_B\} \tag{15}$$

Sample histogram of $\in_B$ values for an ensemble of 10×10 s-boxes is given in
Figure 5, and the relation between $\in_{BIC}$ and n, which we obtain experimentally [5, 6] by considering different ensembles of $n \times n$ s-boxes, is shown in Figure 6. Again, as n gets larger, the maximum correlation $\in_{BIC}$ in an ensemble of 10,000 randomly created s-boxes gets smaller. It is observed from Figure 6 that, for s-boxes of size 16x16, all the $BIC(\boldsymbol{f})$ values in the ensemble fall below 2.6%.

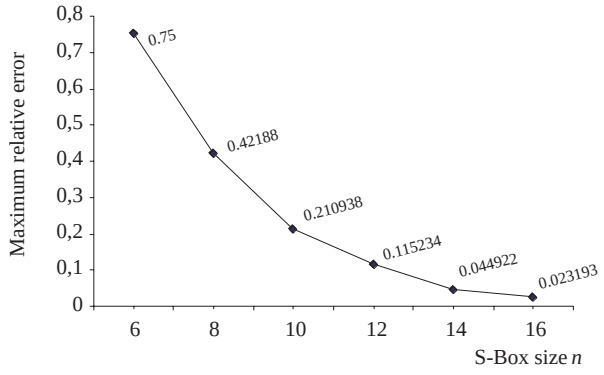


Figure 4. Maximum relative error $\in_{SAC}$ versus s-box size n

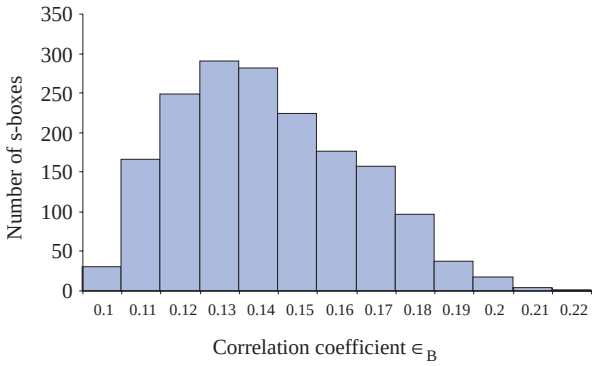
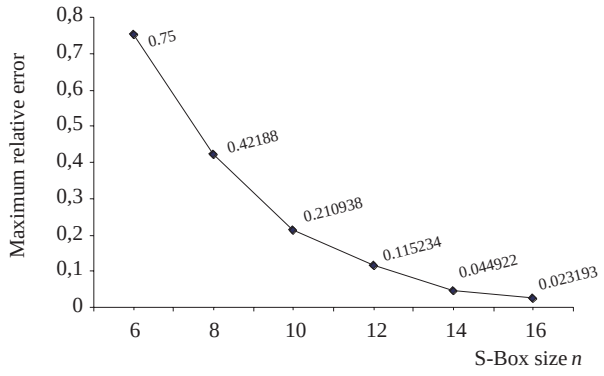


Figure 5. Histogram for correlation coefficients $\in_B$ of BIC for $n = 10$



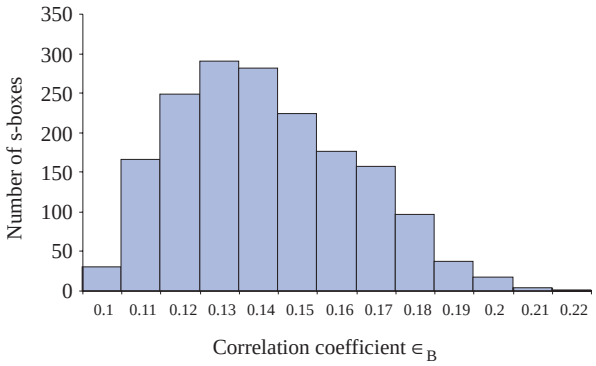


Figure 6. Maximum correlation $\in_{BIC}$ versus n

4. Correlations Among Criteria

In this section we measure the correlations among mentioned criteria, to find out whether or not they indicate different cryptographic aspects of a given s-box. We conjecture that, if the relative error values, $\in_{A,}\in_S$ and $\in_B$, are found to be highly correlated to each other, then it is sufficient to test the cipher for only one of these criteria, and the use of the other two criteria becomes meaningless.

Thus, in order to measure the correlation between each pair of criteria, we compute the absolute correlation coefficient between corresponding relative errors. All coefficients are computed similarly. For instance, the absolute value of the correlation coefficient between the SAC and the BIC (with relative errors $\in_S$ and $\in_B$) is given by

$$C_{SB} = \left| \frac{(\frac{1}{N} \sum_{ensemble} \in_S - \overline{\in_S})(\frac{1}{N} \sum_{ensemble} \in_B - \overline{\in_B})}{\sqrt{\left[\frac{1}{N} \sum_{ensemble} (\in_S^2) - \overline{\in_S}^2\right]\left[\frac{1}{N} \sum_{ensemble} (\in_B^2) - \overline{\in_B}^2\right]}} \right| \tag{16}$$

where N is the total number of $n \times n$ s-boxes in the ensemble. If C_{AS}, C_{AB} and C_{SB} denote the absolute correlation coefficients between the $AVAL$ criterion and the SAC, between the $AVAL$ criterion and the BIC,

and between the SAC and the BIC respectively, our results show that:

i) C_{AS} values are larger than C_{AB} and C_{SB} for all n. (This is an expected result since the SAC is a special form of the the $AVAL$ criterion, so those two criteria should be somewhat correlated.) However, correlation between the SAC and the $AVAL$ is not larger than 25% , and C_{AS} values decrease from 25% to about 12% as n is increased from 6 to 12.

ii) C_{AB} values which show the correlation between the criteria of the $AVAL$ and the BIC are less than 1% for all n.

iii) C_{SB} values which show the correlation between the criteria of the SAC and the BIC are less than 3% for all n.

We then conclude that the the $AVAL$ criterion and the BIC are quite uncorrelated with each other, as well as the SAC and the BIC, i.e., testing an s-box for the the $AVAL$ criterion or the SAC does not give much information about how well this s-box satisfies the BIC. Hence, although observing avalanche characteristics of a small sized s-box may give some information about its strict avalanche characteristics, generally it is quite valuable to test s-boxes for the the $AVAL$ criterion, the SAC and the BIC separately.

5. Conclusions

We define the "relative avalanche error", $\in_A$, and the "relative SAC error", $\in_S$, which indicate how close a randomly chosen s-box is, to satisfying the mentioned criteria of $AVAL$ and SAC respectively. We then obtain the maximum relative errors, $\in_{AVAL}$ and $\in_{SAC}$, found in an ensemble of randomly generated $n \times n$ s-boxes, corresponding to the maximum values of the parameters $\in_A$ and $\in_S$ respectively. By a similar interpretation, $\in_{BIC}$, which we define as the maximum of correlation parameters $BIC(\boldsymbol{f})$ in an ensemble of randomly generated $n \times n$ s-boxes, can be found. The results presented in Section 3 give an idea to what degree these properties are satisfied for randomly generated s-boxes of different sizes.

The experiments of this work use ensembles which contains different s-box functions $\boldsymbol{f}(\mathbf{X})$ chosen randomly, with the two restrictions that, the function $\boldsymbol{f}(\mathbf{X})$ is one to one, and $\boldsymbol{f}(\mathbf{X})$ is different from $\mathbf{X}$. Random 10,000 s-boxes of size $n \times n$ are created, and corresponding $\in_{AVAL}, \in_{SAC}$, and $\in_{BIC}$ parameters are evaluated for various values of n. It is observed that randomly chosen s-boxes satisfy the properties better as n gets larger. Examining the results given in the previous section, we see that for n =16, relative errors decrease to very small values less than 5% for all three criteria, namely $AVAL$, SAC and BIC. Deviation from the ideal behaviour seems to be decreasing further for $n \geq 16$. It is not hard to predict that for randomly created s-boxes of much larger sizes, these properties will be satisfied within very low error ranges.

It is also observed by evaluating the absolute correlation coefficients that all the criteria mentioned in this paper test different aspects of the s-boxes. Observing avalanche characteristics of an s-box may give some information about its strict avalanche characteristics, since correlation up to 25% may exist between the $AVAL$ criterion and the SAC for small sized s-boxes, like 6×6. However, the correlation coefficient between the BIC and the $AVAL$ is less than 1% and that between BIC and SAC is less than 3% , for all values of the s-box size n.

References

[1] H. Feistel, "*Cryptography and computer privacy*", Scientific American, Vol.228, No.5, pp.15-23, May 1973.

[2] H. Feistel, W. A. Notz, and J. L. Smith, "*Some cryptographic techniques for machine to machine data communications",* Proc. IEEE, Vol.63, No.11, pp.1545-1554, November 1975.

[3] A. F. Webster and S. E. Tavares, "*On the design of s-boxes",* Advances in Cryptology: Proc. CRYPTO '85, Springer-Verlag, Berlin, pp. 523-534, 1986.

[4] L. Keliher, *Substitution-permutation network cryptosystems using key-dependent s-boxes*, M.S. Thesis, Queen's University, Kingston, Canada, 1997.

[5] I. Vergili, *Statistics* on *Satisfaction of Security Criteria For Randomly Generated S-Boxes,* M.S. Thesis, Middle East Technical University, Turkey, June 2000.

[6] I. Vergili and M. D. Yücel, "*On Satisfaction of Some Security Criteria for Randomly Chosen S-Boxes"*, Proc. 20^{th} Biennial Symp. on Communications, pp.64-68, Kingston, Canada, May 2000.