Performance Metrics Analysis of S-Box for Cryptosystem

1st Jayati Dutta
Dept. of Electrical Engineering
Indian Institute of Technology
Hyderabad, India
ee20resch11009@iith.ac.in

2nd Priyanka Peri
Dept. of Electrical Engineering
Indian Institute of Technology
Hyderabad, India
ee21mtech12002@iith.ac.in

I. System Performance Metrics and Analysis

In this section we define essential metrics for evaluating the efficiency of S-box in cryptosystem.

A. Cryptosystem Analysis of S-Box

1) *Differential analysis:* For a strong cryptosystem, even a small change in the Cipher Key (CK) or Initialization Vector (IV) should lead to a significant alteration in the resulting keystream. This property, known as the system's sensitivity to differential analysis, is quantified as the net bit change rate due to Differential Analysis ($NBCR|_{DA}$). Let J_1 and J_2 represent the keystreams whose CK or IV differs by a single bit, with S denoting the total number of bits in the keystream,

$$D = \begin{cases} 1; & J_1 \neq J_2 \\ 0; & J_1 = J_2 \end{cases} \tag{1}$$

$$NBCR|_{DA} = \frac{D}{S} \times 100\% \tag{2}$$

2) *Linear analysis:* A good cryptosystem should not exhibit linearity. Non-linearity is defined as,

$$ZUC(J_1 + J_2) \neq ZUC(J_1) + ZUC(J_2) \tag{3}$$

where the process of deriving the keystream from the Cipher Key (CK) and Initialization Vector (IV) is denoted as ZUC(.). To assess the non-linearity of this process, we use a measure called the net bit change rate due to Linear Analysis ($NBCR|_{LA}$). This quantifies how much the keystream changes when linear analysis is applied to variations in the CK and IV. Let J_1 and J_2 represent the keystreams with different CK or IV. J_3 is the keystream generated from the addition of two CK and IV. S represents the total number of bits in the keystream,

$$D = \begin{cases} 1; & ZUC(J_3) \neq ZUC(J_1) \oplus ZUC(J_2) \\ 0; & \text{else} \end{cases} \tag{4}$$

$$NBCR|_{LA} = \frac{D}{S} \times 100\% \tag{5}$$

3) *Statistical analysis:* The randomness of plain text and cipher text is measured by calculating entropy and given by,

$$H(x) = -\sum_{i=0}^{n} p(x_i) \log_2 p(x_i) \text{bits} \tag{6}$$

The entropy of a cipher should ideally be closer to 4 because it represents a highly random and unpredictable sequence.

4) *Correlation analysis:* The Correlation Coefficient is the measure of correlation between plain and cipher text. Mathematically, Correlation Coefficient is defined as,

$$\gamma = \frac{\sum_{i=0}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=0}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=0}^{n}(y_i - \bar{y})^2}} \tag{7}$$

where, x is the plain text, $\bar{x}$ is the mean of the plaintext and y is the ciphertext, $\bar{y}$ is the mean of the cipher text. A correlation coefficient that approaches zero suggests that there is a weaker correlation or relationship between plaintext and ciphertext, indicating a lower level of predictability or correlation between the two.