Proceedings of the Pakistan Academy of Sciences 48 (2): 111–115, 2011
Pakistan Academy of Sciences
ISSN: 0377 - 2969

Original Article

Some Analysis of S-box based on Residue of Prime Number

Iqtadar Hussain[1*], Tariq Shah[1], Hasan Mahmood[2], Muhammad Asif Gondal[3] and Usman Younas Bhatti[3]

[1]Department of Mathematics Quaid-i-Azam University, Islamabad, Pakistan
[2]Department of Electronics, Quaid-i-Azam University, Islamabad, Pakistan
[3]Department of Sciences and Humanities, National University of Computer & Emerging Sciences, Islamabad, Pakistan

Abstract: In this article, we will analyze substitution box (S-box) based on residue of prime number for different analysis such as graphical and analytical strict avalanche criterion (SAC), bit independent criterion (BIC), differential approximation probability (DP), linear approximation probability (LP) and nonlinearity. With the help of these results we determine the algebraic and statistical encryption strength and weakness of this S-box.

Keywords: S-box, Graphical SAC, LP, DP, BIC

1. INTRODUCTION

Block cipher is an important branch of cryptography, and Substitution box is the essential constituent of many block ciphers, which is proficient to create confusion in the plaintext during the process of encryption. So, at some extent we can say that the strength of the block cipher mainly depends on S-box, that's why many researchers have shown attention to improve the quality of S-box and develop some analysis to determine the confusion capability of S-box. There are many analysis existing in literature such as graphical and analytical strict avalanche criterion (SAC), bit independent criterion (BIC), differential approximation probability (DP), linear approximation probability (LP) and nonlinearity.

In this letter, we will analyze S-box [1], presented by E. S. Abuelyman and A. A. S. Alsehibani, by some well known analysists which have discussed earlier. This analysis includes nonlinearity, BIC, SAC, LP, DP etc, these criterions are necessary for a good S-box. S-box [1], does not satisfied all criterions entirely but close to the optimal value. So we can use it in encryption for secure communication.

This paper is structured as follows; section 2 present analysis of S-box which includes nonlinearity analysis, bit independent criterion analysis, linear approximation probability analysis, differential approximation probability analysis, analytical strict avalanche criterion analysis, graphical strict avalanche analysis and section 3 presents conclusion.

2. ANALYSES OF S-BOX

In this section, we will present some useful analysis of S-box based on residue of prime number.

2.1. Nonlinearity

The nonlinearity of a Boolean function can be defined as the distance between the function and the set of all affine functions. In other words we can say that, Non-linearity is the number of bits which must be changed in the truth table of a Boolean function to reach the closest affine function. The upper bound of nonlinearity is: $N(f)=2^{n-1}-2^{n/2-1}$ [2], for S-box in $GF(2^n)$. As S-box in AES is in $GF(2^8)$, the optimal value of N is 120.

Table 1. The results of nonlinearity of S-box based on residue of prime number

0	1	2	3	4	5	6	7
94	100	104	104	102	100	98	94

Maximum value=104; Minimum value=94; Average value=99.5

Received July 2010, Accepted June 2011

*Corresponding author: Iqtadar Hussain, Email: iqtadarqau@gmail.com

2.2. Bit Independent Criterion

The output bits independence criterion (BIC) was also first introduced by Webster and Tavares [3] which is another desirable property for any cryptographic design. It means that all the avalanche variables should be pair-wise independent for a given set of avalanche vectors generated by the complementing of a single plaintext bit.

Table 2. The Nonlinearity of BIC of S-box based on residue of prime number.

----	102	104	98	104	98	100	94
102	----	104	98	106	100	100	98
104	104	----	106	104	106	106	106
98	98	106	----	106	100	102	102
104	106	104	106	----	100	100	106
98	100	106	100	100	----	94	100
100	100	106	102	100	94	----	104
94	98	106	102	106	100	104	----

Table 3. The dependent matrix in BIC of S-box based on residue of prime number.

---	0.539	0.498	0.519	0.498	0.498	0.478	0.501
0.539	----	0.521	0.531	0.470	0.490	0.486	0.531
0.498	0.521	----	0.503	0.523	0.492	0.486	0.509
0.519	0.531	0.503	----	0.494	0.500	0.490	0.496
0.498	0.470	0.523	0.494	----	0.509	0.488	0.505
0.498	0.490	0.492	0.500	0.509	----	0.533	0.476
0.478	0.486	0.486	0.490	0.488	0.533	----	0.507
0.501	0.531	0.509	0.496	0.505	0.476	0.507	----

From Table 2 and 3 we can observe that S-box [1] satisfied bit independent criterion close to the best possible value.

2.3. Linear Approximation Probability

The linear approximation probability is the maximum value of the imbalance of an event. The parity of the input bits selected by the mask Γx is equal to the parity of the output bits selected by the mask Γy. According to Matsui's original definition [4], linear approximation probability (or probability of bias) of a given s-box is defined as,

$$LP = \max_{\Gamma x, \Gamma y \neq 0} \left| \frac{\#\{x / x \bullet \Gamma x = S(x) \bullet \Gamma y\}}{2^n} - \frac{1}{2} \right|$$

Where Γx and Γy are input and output masks, respectively; X is the set of all possible inputs; and 2n is the number of its elements.

We have calculated the linear approximation probability of S-box [1]. The maximum value of LP is 0.1328.

2.4. Differential Approximation Probability

The nonlinear transformation S-box should ideally have differential uniformity. An input differential Δx_i should uniquely map to an output differential $y_{i,}$ thereby ensuring a uniform mapping probability for each i. The differential approximation probability of a given S-box (i.e., DPs) is a measure for differential uniformity and is defined as

$$DP^{s}(\Delta x \to \Delta y) = \left[\frac{\#\{x \in X / S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^m} \right]$$

Table 4. The differential approximation probability of S-box based on residue of prime number.

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0.031	0.023	0.023	0.031	0.023	0.031	0.023	0.039	0.031	0.031	0.031	0.031	0.023	0.031	0.023	0.039
0.023	0.023	0.023	0.031	0.023	0.039	0.023	0.039	0.031	0.031	0.031	0.031	0.031	0.031	0.023	0.039
0.031	0.023	0.023	0.031	0.047	0.023	0.023	0.039	0.039	0.031	0.031	0.031	0.031	0.031	0.023	0.039
0.047	0.031	0.023	0.039	0.023	0.023	0.023	0.031	0.039	0.031	0.023	0.031	0.031	0.031	0.023	0.039
0.031	0.031	0.031	0.031	0.023	0.016	0.023	0.031	0.031	0.023	0.031	0.023	0.031	0.023	0.023	0.031
0.047	0.023	0.031	0.031	0.031	0.023	0.039	0.031	0.031	0.031	0.023	0.023	0.023	0.031	0.031	0.031
0.039	0.031	0.023	0.031	0.031	0.031	0.023	0.039	0.047	0.031	0.031	0.039	0.031	0.031	0.016	0.031
0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.047	0.023	0.031	0.023	0.031
0.039	0.031	0.023	0.031	0.023	0.031	0.039	0.031	0.023	0.023	0.031	0.039	0.047	0.023	0.023	0.031
0.047	0.023	0.023	0.031	0.023	0.031	0.031	0.023	0.023	0.031	0.023	0.031	0.031	0.023	0.023	0.031
0.031	0.031	0.031	0.031	0.031	0.023	0.039	0.031	0.031	0.031	0.023	0.047	0.031	0.031	0.031	0.031
0.031	0.031	0.031	0.039	0.023	0.031	0.023	0.039	0.047	0.023	0.023	0.031	0.031	0.023	0.023	0.023
0.031	0.031	0.023	0.031	0.031	0.023	0.023	0.031	0.039	0.023	0.023	0.039	0.031	0.023	0.023	0.031
0.031	0.031	0.023	0.031	0.031	0.023	0.023	0.047	0.031	0.023	0.031	0.023	0.031	0.023	0.023	0.031
0.039	0.023	0.023	0.031	0.031	0.031	0.023	0.031	0.039	0.023	0.023	0.023	0.039	0.031	0.031	0.023
0.047	0.031	0.031	0.023	0.031	0.031	0.023	0.031	0.125	0.023	0.023	0.023	0.281	0.023	0.031	------

The maximum value of differential approximation probability for S-box [1] is also 0.2812 (see Table-4).

2.5. Strict Avalanche Criterion Analytically

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.

More formally a function $f : F_2^n \rightarrow F_2$ satisfies SAC if $f(x) \oplus f(x \oplus \alpha)$ is balanced for all α whose weight is 1.

Table 5. The results of Strict avalanche criterion for S-box based on residue of prime number.

0.343	0.671	0.515	0.468	0.468	0.546	0.437	0.5
0.562	0.468	0.468	0.437	0.531	0.453	0.453	0.484
0.562	0.531	0.437	0.546	0.39	0.468	0.593	0.531
0.562	0.515	0.578	0.437	0.421	0.625	0.531	0.531
0.609	0.484	0.453	0.468	0.64	0.531	0.515	0.578
0.593	0.421	0.5	0.578	0.515	0.5	0.578	0.625
0.468	0.453	0.562	0.484	0.515	0.562	0.609	0.578
0.421	0.5	0.484	0.515	0.562	0.578	0.593	0.468

Minimum value=0.343; Maximum value=0.671; Average value= 0.516; Square deviation=0.032

The results in Table 4 shows that the value of strict avalanche criterion of S-box based on residue of prime number is ~1/2.

2.6. Strict Avalanche Criterion Graphically

Mar and Latt [5] have given the following three graphical methods to analyze strict avalanche criterion (SAC):

1) Analysis of Frequency of various Hamming weight.
2) Analysis of Differential Values.
3) Analysis of Hamming Weight According to Bit Position.

Analysis of Frequency of various Hamming Weight

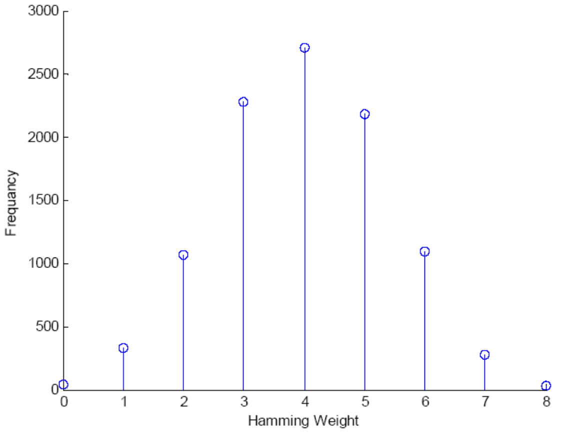

Fig. 1. Analysis of various Hamming weight for Residue prime number S-box

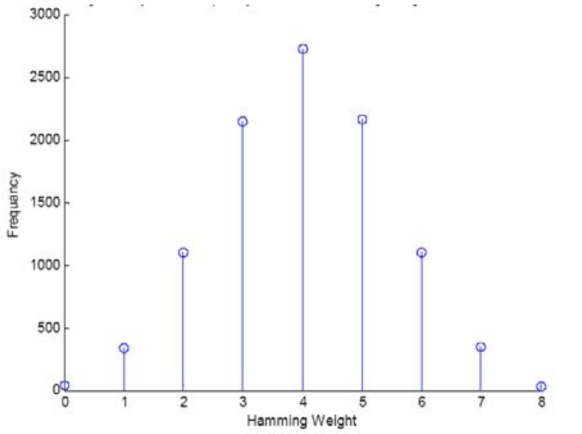

Fig. 2. Analysis of frequency of various Hamming weight for AES S-box

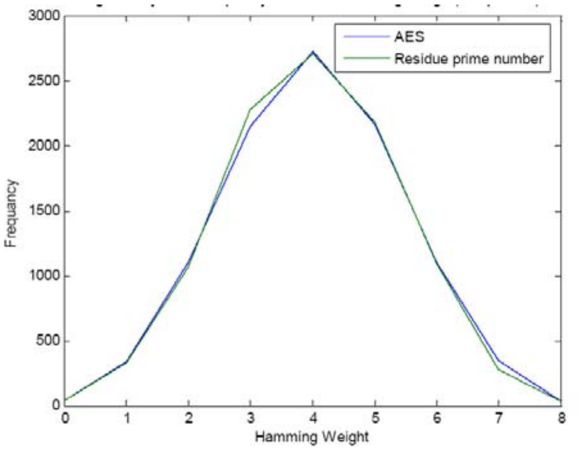

Fig. 3. Analysis of frequency of various Hamming weights (Comparison)

Fig.1, 2 and 3 show the analysis of frequency of various Hamming weights for S-box [1], AES S-box [6], and their comparison. By comparing the graph of S-box [1], with frequency of various Hamming weights of standard graph of [5], we analyzed that residue prime number S-box [1], satisfies the condition of good S-box.

Analysis of Differential values

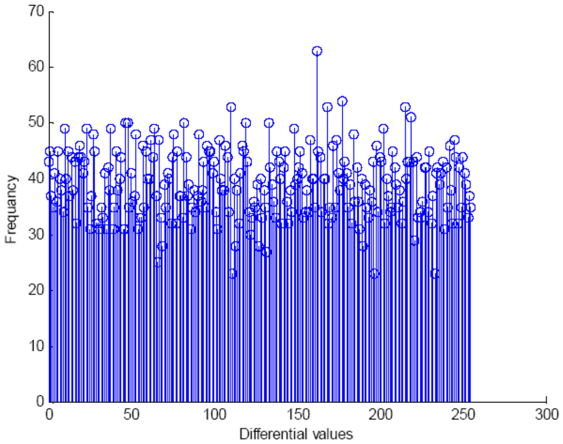

Fig. 4. Analysis of differential values for Residue prime number S-box.

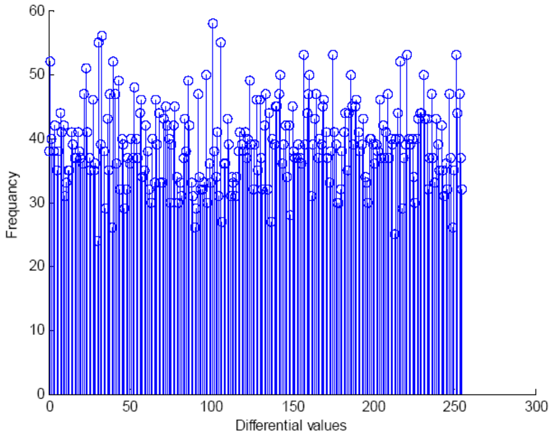

Fig. 5. Analysis of differential values for AES S-box.

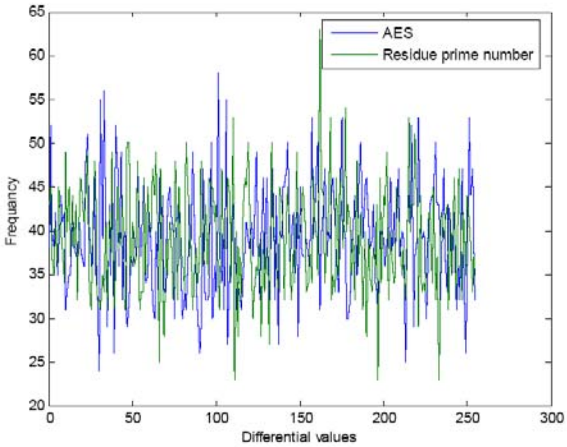

Fig. 6. Analysis of differential values (Comparison

Fig. 4, 5 and 6 show the analysis of differential values of S-box [1], AES S-box [6], and their comparison. If we compare the graph S-box [1], with differential values of standard graph of [5], we analyze that residue prime number S-box[1] does not satisfy the conditions of good S-box but these three graphs show that the completeness property of residue prime number S-box is similar with AES S-box [6] .

Analysis of Hamming Weight According to Bit Position

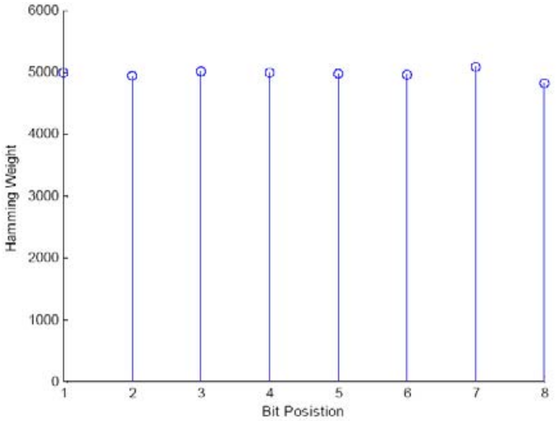

Fig. 7. Analysis of Hamming weight according to bit position for residue of prime number S-box.

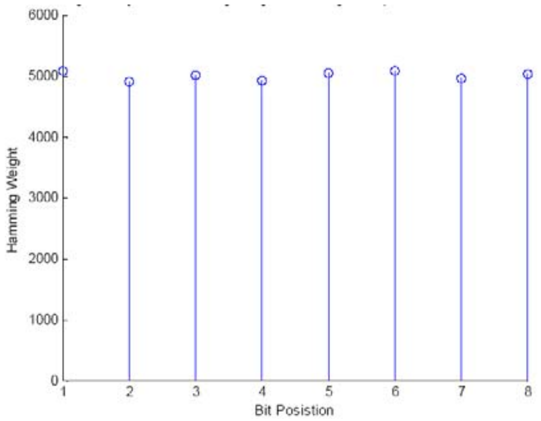

Fig. 8. Analysis of Hamming weight according to bit position for AES S-box.

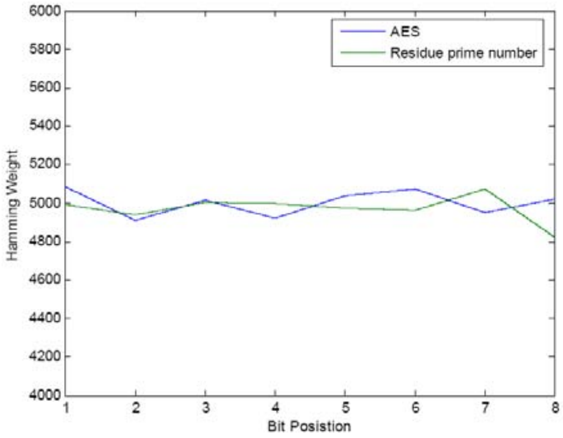

Fig. 9. Analysis of Hamming weight according to bit position (Comparison).

Fig-7, 8 and 9 shows the analysis of Hamming weight according to bit position of S-box [1], AES S-box [6] and their comparison. If we compare the graph of residue prime number S-box [1] with Hamming weight according to bit position of standard graph [5], we analyze that residue prime number S-box satisfies the conditions of good S-box and these graphs show that this S-box fulfills the condition of strong S-box.

3. CONCLUSION

In this paper, we analyzed S-box for different criteria as described above, and bring to a close that S-box based on residue of prime number does not satisfy all criteria absolutely but the analysis results are up to the standard. Particularly, the results of Strict Avalanche Criterion are very close to optimal value, so this S-box can be used in encryption for secure communication.

4. REFERENCES

1. Abuelyman, E.S. & A.A.S. Alsehibani. An optimized implementation of the S-Box using residue of prime numbers. *International Journal of Computer Science and Network Security,* 8: 304-309 (2008).
2. Feng, D. & W. Wu. *Design and Analysis of Block Ciphers.* Tsinghua University Press (2000).
3. Detombe, J. & S. Tavares. *Constructing Large Cryptographically Strong S-boxes*: *Advances in Cryptology,* Proc. of CRYPTO92, Lecture Notes in Computer Science. p. 165-181 (1992).
4. Matsui, M. *Linear cryptanalysis method of DES cipher*: *Advances in Cryptology,* Proceeding of the Eurocrypt’93, Lecture Notes in Computer Science 765, p. 386-397 (1994).
5. Mar, P.P. & K.M. Latt. New analysis methods on strict avalanche criterion of Sboxes. *World Academy of Science, Engineering and Technology,* 48: 150-154 (2008).
6. Daemen, J. & V. Rijmen. *The Design of RIJNDAEL: AES- The Advanced Encryption Standard.* Springer-Verlag, Berlin (2002).
7. Hussain I, T. Shah & H. Mahmood . A New Algorithm to Construct Secure Keys for AES. *International Journal of Contemporary Mathematical Sciences,* 5(26): 1263-1270 (2010).