Comparative Analysis of S-boxes Based on Graphical SAC

Iqtadar Hussain
Quaid-i-Azam University
Department of Mathematics
Quaid-i-Azam University, Islamabad
Pakistan

Tariq Shah
Quaid-i-Azam University
Department of Mathematics
Quaid-i-Azam University, Islamabad
Pakistan

Hasan Mahmood
Quaid-i-Azam University
Department of Electronics
Quaid-i-Azam University, Islamabad
Pakistan

Mehreen Afzal
Department of Information Security
Military College of Signals, NUST,
Pakistan

ABSTRACT

Substitution box (S-box) is generally the only non-linear component of block cipher. That is why; security of a cipher is centralized on the characteristics of an S-box, which are measure of its resistance against different cryptanalytic techniques. In this regard, it is important to investigate the new designs of S-boxes for these characteristics. In this letter we analyze AES, APA, Gray, Lui J and Graph Isomorphism S-boxes for graphically Strict Avalanche Criterion and also observe that how close these S-boxes are to the original AES in these analyses.

Keywords

AES, APA, Gray, Lui J, Graph Isomorphism S-boxes and Strict Avalanche Criterion (SAC)

1. INTRODUCTION

S-box of a block cipher, that can also be viewed as a n × m mapping: $S : F_2^n \to F_2^m$, is designed according to the principles laid down by Shannon (1949) in [1]. Webster and Tavares (1986) in [2] gave the idea of strict avalanche criteria (SAC) by combining the effects of completeness and avalanche effect. SAC characterizes the output when there is a change in input bits of an S-box.

In this article we aim at investigating SAC, with the graphical analysis techniques developed by Mar and Latt in [3], of some newly proposed S-box designs [4], [5], [6], [7].

In [4], Affine-Power-Affine (APA) S-box for Advanced Encryption Standard has been presented. Design of APA S-box aims at enhancing the algebraic complexity of Rijndael's
S-box [8], from 9 to 253 terms. Thus, the algebraic complexity can be increased with Affine Power Affine structure.

In [5], Gray S-box construction is discussed in which binary Gray code transformation is added as a preprocessing step to original AES S-box. Gray S-box corresponds to a polynomial with all 255 non-zero terms in comparison with 9-term polynomial of original AES S-box. This also increases the security for S-box against algebraic attacks and interpolation attacks. Besides, as Gray S-box reuses AES S-box as a whole, therefore all advantages and efficiency of any existing optimized implementation of AES S-box are also inherited.

The construction presented in [7], also aims at increasing the complexity of Algebraic expression of Rijndael's S-box to 255 terms. They achieve this by adding a linear transformation built on graph isomorphism. Yet another construction given in [6] also increases the terms of AES S-box to 255 by changing the order of linear and inverse transformations.

This paper is structured as follows. In next section, we analyze graphically APA, Gray, Lui J and graph isomorphism based S-boxes for strict avalanche criterion and also compare these results with AES S-box. We present the conclusion in Section 3.

2. ANALYSIS OF S-BOXES

An S-box satisfies SAC if a change in a single bit on the input results in a change on half of the output bits. More formally, a function $f : F_2^n \to F_2$ satisfies the Strict Avalanche Criterion if $f(x) \oplus f(x+\alpha)$ is balanced $\forall \alpha$.

We present graphical analysis of SAC of S-boxes, using three methods developed by Mar and Latt in [3]. These methods include analysis of frequency of various Hamming weights, analysis of differential values, and analysis of Hamming weights according to bit position.

2.1 Analysis of Frequency of Various Hamming weights

Using this method, frequency of different Hamming weights is counted for differential value $\Delta y = y \oplus y'$. Where $y = S(x)$ and $y' = S(x')$. Here, $x, x' \in Z_2^m$ are two random inputs of the S-box $S : Z_2^n \to Z_2^m$. Figure 1 presents a comparison of the frequency of Hamming weights for APA, Gray, Lui J and graph isomorphism based S-box constructions.

2.2 Analysis of Differential Values

In this method, frequencies of different differentials are counted for random input values. A comparison of S-boxes under our investigation based on this method is presented in Figure 2.

2.3 Analysis of Hamming Weights According to Bit Position

In this method, frequencies of hamming weights of different differentials are counted according to different bit positions for random input values. A comparison of S-boxes under our investigation based on this method is presented in Figure 3.

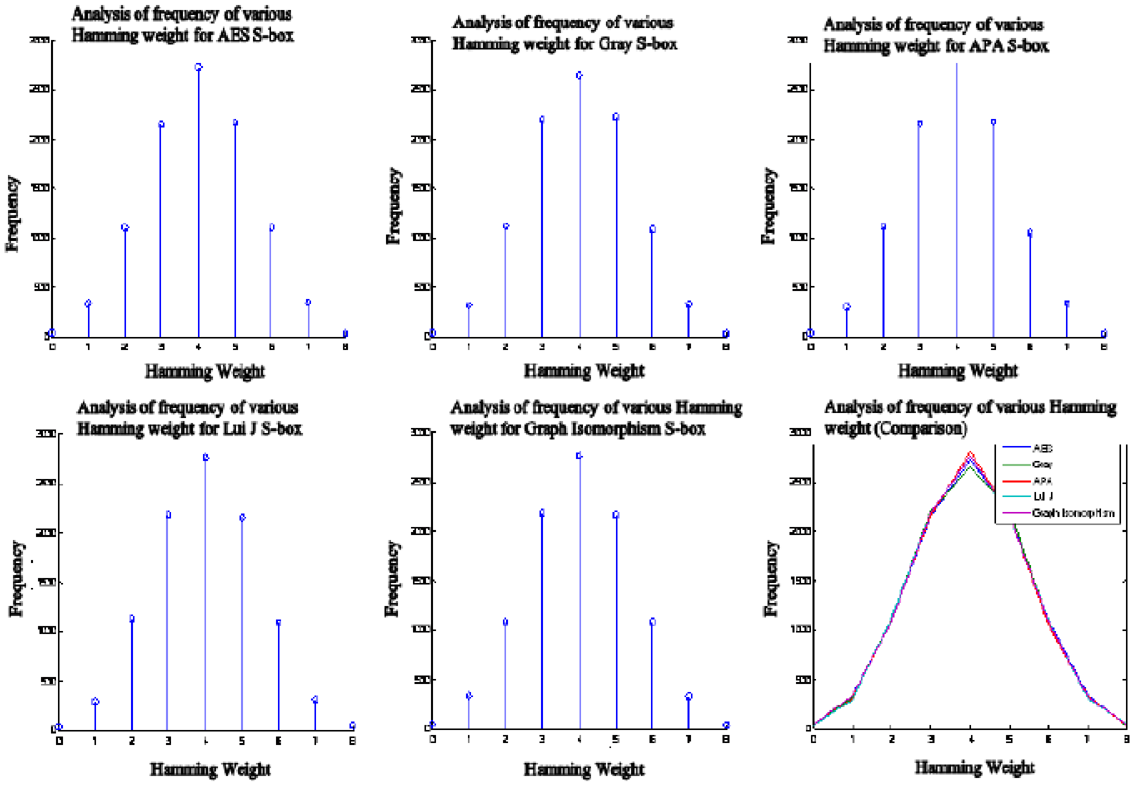

Figure 1: A Comparison of Frequency of Various Hamming Weight for different S-boxes

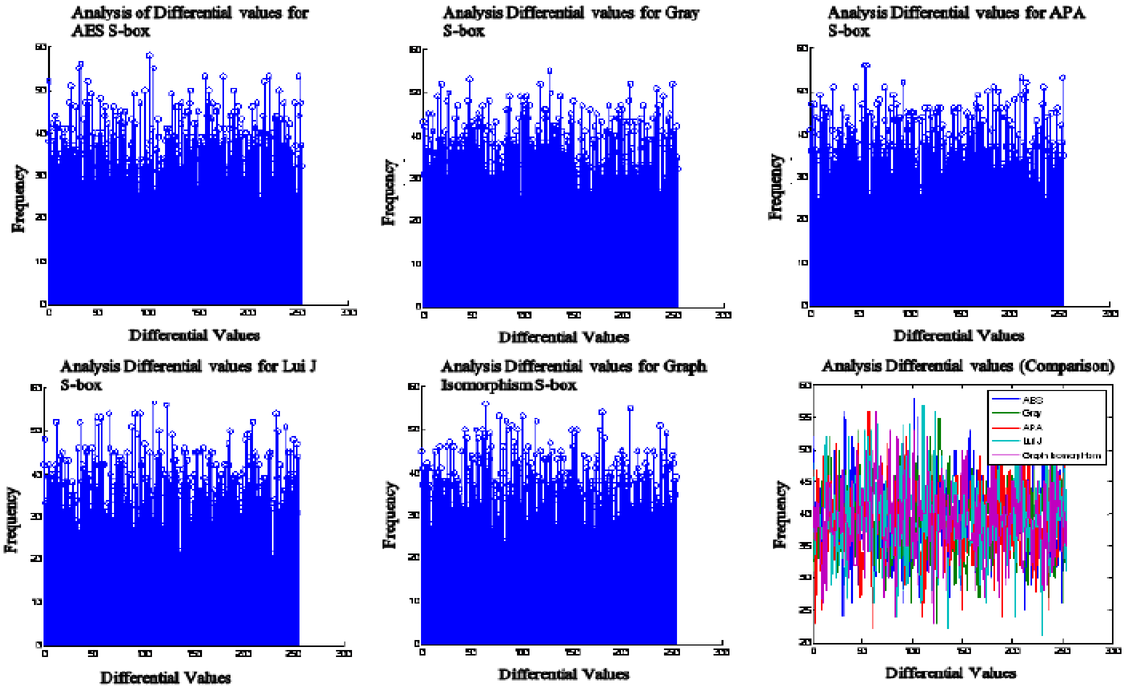

Figure 2: A Comparison of Frequency of Differentials for different S-boxes

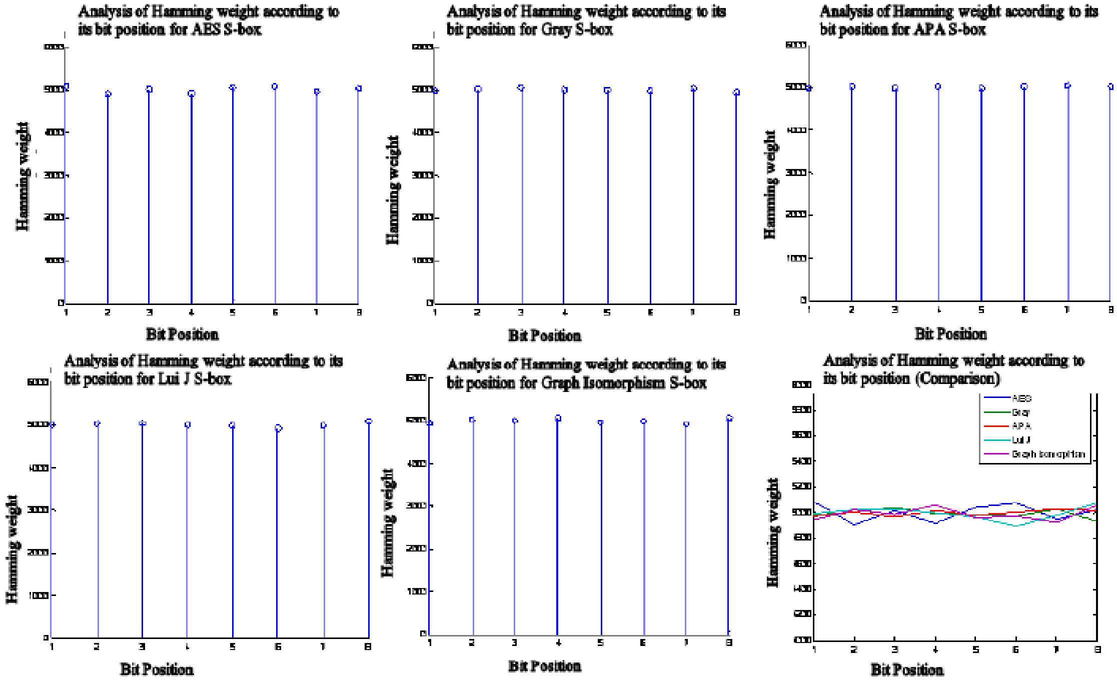

Figure 3: A Comparison of Hamming Weights According to Bit Position for Different S-boxes

3. CONCLUSION

In this letter, we analyze Gray, APA, Lui J and Graph Isomorphism based S-boxes for graphical strict avalanche criterion, and compare the results with the original AES S-box characteristics. We conclude that all S-boxes satisfy the Strict Avalanche Criterion for good S-boxes. With this analysis, we can see which S-box satisfies strict avalanche criterion and how much it is close to the optimal values.

4. ACKNOWLEDGMENTS

This work is supported in part by HEC Grant No. 1-308/ILPUFU/HEC/2009.

5. REFERENCES

1. Shannon, C. E. 1949. Communication theory of secrecy systems. Bell System Technical Journal 28-4, pp. 656–715.
2. Webster A. and Tavares. S. 1986. On the design of S-boxes. In: Advances in Cryptology-Eurocrypt'85. Lecture Notes in Computer Science. Springer Verlag, pp. 523–534.
3. Mar P. and Latt. M. 2008. New analysis methods on strict avalanche criterion of S-boxes, World Academy of Science 48. pp.150-154.
4. Cui L. and Cao. Y. 2007. A new S-box structure named affine-power-affine. International Journal of Innovative Computing, Information and Control 3, pp. 751–759.
5. Tran T. and Doung B. 2008. Gray S-box for advanced encryption standard. In: International Conference on Computational Intelligence and Security. pp. 253–256.
6. Liu J, Wai. B. and Wang C. 2005. An AES S-box to increase complexity and cryptographic analysis. In: 19th International Conference on Advanced Information Networking and Applications (AINA.05). Vol. 1. pp. 724–728.
7. Tran B. N, Nguyen. T. D and Tran T. D. 2009. A new S-box structure based on graph isomorphism. In: International Conference on Computational Intelligence and Security. pp.463-467.
8. Daemen J. and Rijmen V. 1999. AES proposal: Rijndael AES algorithm submission.