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.

Reference


Index Terms

Computer Science Security

Key words

AES
APA

Gray

Lui J

Graph Isomorphism S-boxes

Strict Avalanche Criterion (SAC)