World Academy of Science, Engineering and Technology
International Journal of Electrical and Computer Engineering
Vol:11, No:04, 2017

Open Science Index, Electrical and Computer Engineering Vol:11, No:04, 2017 publications.waset.org/abstracts/65017.pdf

Classifying and Analysis 8-Bit to 8-Bit S-Boxes Characteristic Using S-Box Evaluation Characteristic

Authors : Muhammad Luqman, Yusuf Kurniawan

Abstract : S-Boxes is one of the linear parts of the cryptographic algorithm. The existence of S-Box in the cryptographic algorithm is needed to maintain non-linearity of the algorithm. Nowadays, modern cryptographic algorithms use an S-Box as a part of algorithm process. Despite the fact that several cryptographic algorithms today reuse theoretically secure and carefully constructed S-Boxes, there is an evaluation characteristic that can measure security properties of S-Boxes and hence the corresponding primitives. Analysis of an S-Box usually is done using manual mathematics calculation. Several S-Boxes are presented as a Truth Table without any mathematical background algorithm. Then, it’s rather difficult to determine the strength of Truth Table S-Box without a mathematical algorithm. A comprehensive analysis should be applied to the Truth Table S-Box to determine the characteristic. Several important characteristics should be owned by the S-Boxes, they are Nonlinearity, Balancedness, Algebraic degree, LAT, DAT, differential delta uniformity, correlation immunity and global avalanche criterion. Then, a comprehensive tool will be present to automatically calculate the characteristics of S-Boxes and determine the strength of S-Box. Comprehensive analysis is done on a deterministic process to produce a sequence of S-Boxes characteristic and give advice for a better S-Box construction.

Keywords : cryptographic properties, Truth Table S-Boxes, S-Boxes characteristic, deterministic process

Conference Title : ICHDSIA 2017 : International Conference on Homeland Defense and Security Information Analysis

Conference Location : Zurich, Switzerland

Conference Dates : April 20-21, 2017