# Analysis of avalanche effect on advance encryption standard by using dynamic S-Box depends on rounds keys

## ABSTRACT

Substitution table or S-Box is the major core of AES algorithm and it is used to provide confusion capability for AES. The aim of this paper is to design dynamic S-Box which depends on rounds keys for encryption in AES-128. The parameters of the dynamic S-Box have features equivalent to those in the normal algorithm AES. Static S-Box allows attackers to study S-Box and discover weak issues while by using dynamic S-Box approach, it makes difficult and more complex for attacker to do any offline study of an attack of one particular set of S- boxes. Both algorithms are implemented with MATLAB and also, input and output for data collection is hexadecimal format. the proposed AES is compared with normal AES in term of security analysis by avalanche effect test, and it is compared simulation times between two algorithms.

**Keyword:** Advance encryption standard; AES; Avalanche effect; Dynamic S-Box