A proposal for improving AES S-box with rotation and key-dependent

ABSTRACT

In this paper, a new AES-like design for key-dependent AES using S-box rotation is proposed. We also show how this property can be used to make the S-box key-dependent hence make the AES stronger. The cipher structure resembles the original AES, only the S-box is made key-dependent without changing the value. This new design is tested using the NIST Statistical Test and will be further cryptanalyzed with algebraic attack in order to permit its subversion or evasion.

Keyword: AES; Cryptanalysis; Inverse S-box; Key-dependent S-box