Abstract

The Data Encryption Standard (DES) is the most widely used cryptosystem developed by a team of cryptographers working at IBM. DES has been cryptanalyzed intensively by researchers, but no efficient attack has been found on DES so far. This is mainly due to the lack of an obvious algebraic relation in the structure of S-boxes, which makes it impossible to use known methods to attack DES. S-boxes are the nonlinear part of DES with strong properties. This paper presents a semi-linear relation between input and output of S-boxes that could be used to cryptanalyze DES. This is based on Differential Cryptanalysis method proposed by Biham and Shamir.

References

- E. Biham, A. Shamir, 1991. Differential Cryptanalysis of DES-like Cryptosystems,
A Semi-Linear Relation between Inputs and Outputs of DES S-Boxes


Index Terms

Computer Science  Security

Keywords
- DES  S-Box  Differential Cryptanalysis