Abstract

Differential Cryptanalysis is a powerful technique in cryptanalysis, applied to symmetric-key block ciphers. It is a chosen plain-text attack which means the cryptanalyst has some sets of the plain-text and the corresponding cipher-text pairs of his choice. These pairs of the plain-text are related by a constant difference. Basically it is the study of how differences in input information can affect the resultant difference at the output.

In this paper, differential cryptanalysis is applied on substitution-permutation network and data encryption standards cipher. The survey is based on the analysis of a simple, yet realistically structured, basic Substitution-Permutation Network cipher. Along with this, the paper also presents our contribution in this paper as well as our future research work.
References


Index Terms
Differential Cryptanalysis on Block Ciphers: New Research Directions

Keywords

Differential Cryptanalysis, Symmetric Key, Substitution Permutation Network (SPN), Security, Differential Attack