Abstract

Block cipher is in vogue due to its requirement for integrity, confidentiality and authentication. Differential and Linear cryptanalysis are the basic techniques on block cipher and till today many cryptanalytic attacks are developed based on these. Each variant of these have different methods to find distinguisher and based on the distinguisher, the method to recover key. This paper illustrates the steps to find distinguisher and steps to recover key of all variants of differential and linear attacks developed till today. This is advantageous to cryptanalyst and cryptographer to apply various attacks simultaneously on any crypto algorithm.

References

22. E. Biham, O. Dunkelman, N. Keller, "New Results and boomerang and rectangle attack,"
Variants of Differential and Linear Cryptanalysis


Index Terms

Computer Science

Security

Keywords

Boomerang, Differential Cryptanalysis, Higher Order, Impossible, Integral, Linear cryptanalysis, Rectangle, Related Key, Truncated, Zero Correlation