Current Trends in Linear Cryptanalysis

Kaisa Nyberg

The linear cryptanalysis method presented by M. Matsui in 1993 has evolved to a powerful and flexible method for assessing the security of block ciphers. Today it comes in several variations and extensions and has been applied to multiple of ciphers. After presenting the method in its full generality we will present some examples of its recent applications to concrete ciphers such as the analysis of Ashur et al. of Speck and the multivariate method by Vejre et al. on PRESENT. We will also discuss some caveats due to dependencies between linear approximations encountered in these analyses and present methods to work around them.