

In this thesis, we explain the term CCZ-equivalence in more detail together with an analysis of a special type of matrices of this equivalence. We also clarify the higher order differential cryptanalysis and its generalized version. To demonstrate this method we present several attacks on a simple five round Feistel cipher, two of these attacks are our own. We have implemented the most important attacks and results of these experiments can be found in the text. We also explore how to use a decomposition $F = F_2 \circ F_1^{-1}$ (where F_1 and F_2 are permutations) to construct a generalized higher order differential attack to a block cipher with an S-box F . This construction may be used while searching for an attack to F using the CCZ-equivalence which is generally a hard question. The result of our research is a theorem which presents a necessary condition on a degree of F which is needed for an existence of such a decomposition.