Known and chosen key differential distinguishers for block ciphers.

Summary: In this paper we investigate the differential properties of block ciphers in hash function modes of operation. First we show the impact of differential trails for block ciphers on collision attacks for various hash function constructions based on block ciphers. Further, we prove the lower bound for finding a pair that follows some truncated differential in case of a random permutation. Then we present open-key differential distinguishers for some well known round-reduced block ciphers.

For the entire collection see [Zbl 1225.68026].

MSC:

94A60 Cryptography

Keywords:

block cipher; differential attack; open-key distinguisher; Crypton; Hierocrypt; SAFER++; Square

Full Text: DOI