World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:11, No:06, 2017

Improved Impossible Differential Cryptanalysis of Midori64

Authors : Zhan Chen, Wenquan Bi, Xiaoyun Wang

Abstract : The Midori family of light weight block cipher is proposed in ASIACRYPT2015. It has attracted the attention of numerous cryptanalysts. There are two versions of Midori: Midori64 which takes a 64-bit block size and Midori128 the size of which is 128-bit. In this paper an improved 10-round impossible differential attack on Midori64 is proposed. Pre-whitening keys are considered in this attack. A better impossible differential path is used to reduce time complexity by decreasing the number of key bits guessed. A hash table is built in the pre-computation phase to reduce computational complexity. Partial abort technique is used in the key seiving phase. The attack requires 259 chosen plaintexts, 214.58 blocks of memory and 268.83 10-round Midori64 encryptions.

Keywords : cryptanalysis, impossible differential, light weight block cipher, Midori
Conference Title : ICICS 2017 : International Conference on Information and Communications Security
Conference Location : San Francisco, United States
Conference Dates : June 07-08, 2017