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

11-Round Impossible Differential Attack on Midori64

Authors : Zhan Chen, Wenquan Bi

Abstract : This paper focuses on examining the strength of Midori against impossible differential attack. The Midori family of light weight block cipher orienting to energy-efficiency is proposed in ASIACRYPT2015. Using a 6-round property, the authors implement an 11-round impossible differential attack on Midori64 by extending two rounds on the top and three rounds on the bottom. There is enough key space to consider pre-whitening keys in this attack. An impossible differential path that minimises the key bits involved is used to reduce computational complexity. Several additional observations such as partial abort technique are used to further reduce data and time complexities. This attack has data complexity of 2 $^{69.2}$ chosen plaintexts, requires 2 $^{14.58}$ blocks of memory and 2 $^{94.7}$ 11- round Midori64 encryptions.

Keywords : cryptanalysis, impossible differential, light weight block cipher, Midori
Conference Title : ICISC 2017 : International Conference on Information Security and Cryptography
Conference Location : Amsterdam, Netherlands
Conference Dates : June 18-19, 2017

Open Science Index, Information and Communication Engineering Vol:11, No:06, 2017 publications.waset.org/abstracts/67242.pdf