Finding Integral Distinguishers with Ease

The division property method is a technique to determine integral distinguishers on block ciphers. While the complexity of finding these distinguishers is higher, it has recently been shown that MILP and SAT solvers can efficiently find such distinguishers. In this paper, we provide a framework to automatically find those distinguishers which solely requires a description of the cryptographic primitive. We demonstrate that by finding integral distinguishers for 30 primitives with different design strategies. We provide several new or improved bit-based division property distinguishers for ChaCha, Chaskey, DES, GIFT, LBlock, Mantis, Qarma, RoadRunner, Salsa and SM4. Furthermore, we present an algorithm to find distinguishers with lower data complexity more efficiently.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Department of Mechanical Engineering, Ferdowsi University of Mashhad, Cybercrypt A/S
Corresponding author: Kölbl, S.
Contributors: Eskandari, Z., Kidmose, A. B., Kölbl, S., Tiessen, T.
Pages: 115-138
Publication date: 1 Jan 2019

Host publication information
Title of host publication: Selected Areas in Cryptography – SAC 2018
Publisher: Springer
Editors: Cid, C., Jacobson, M. J.
ISBN (Print): 9783030109691
(Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 11349 LNCS).
Keywords: Division property, Integral attacks, Tool
DOIs: 10.1007/978-3-030-10970-7_6
Source: Scopus
Source-ID: 85060711382
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2019 › Research › peer-review