README

This folder contains source codes of the paper titled 'Accelerating the Search of Differential and Linear Characteristics with the SAT Method'

Ling Sun[1,2], Wei Wang[1,2] and Meiqin Wang[1,2](✉)

[1] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China
[2] School of Cyber Science and Technology, Shandong University, Qingdao, China
lingsun@sdu.edu.cn, weiwangsdu@sdu.edu.cn, mqwang@sdu.edu.cn

Abstract. This folder includes source codes of the paper titled 'Accelerating the Search of Differential and Linear Characteristics with the SAT Method'. The SAT solver CaDiCaL must be installed before the implementation of the program.

Keywords: No keywords given.

- The folder `1.Source-Code` contains source codes of some ciphers.
  - `1.PRESENT`
    - `1.Differential-Active-Sbox/SearchWithCadical.py` is the program to search for the optimal differential trail with the minimum number of active S-boxes.
    - `2.Differential-Probability/SearchWithCadical.py` is the program to search for the optimal differential trail with the maximum probability.
    - `3.Linear-Active-Sbox/SearchWithCadical.py` is the program to search for the optimal linear trail with the minimum number of active S-boxes.
    - `4.Linear-Bias/SearchWithCadical.py` is the program to search for the optimal linear trail with the maximum correlation.
  - `2.LBlock`
    - `1.Differential-Active-Sbox/SearchWithCadical.py` is the program to search for the optimal differential trail with the minimum number of active S-boxes.
    - `2.Differential-Probability/SearchWithCadical.py` is the program to search for the optimal differential trail with the maximum probability.
    - `3.Linear-Active-Sbox/SearchWithCadical.py` is the program to search for the optimal linear trail with the minimum number of active S-boxes.
    - `4.Linear-Bias/SearchWithCadical.py` is the program to search for the optimal linear trail with the maximum correlation.
  - `3.SIMON`
    - `1.Differential-Probability/SearchWithCadical.py` is the program to search for the optimal differential trail with the maximum probability.
    - `2.Linear-Bias/SearchWithCadical.py` is the program to search for the optimal linear trail with the maximum correlation.