README

This folder contains all auxiliary materials of the paper titled 'On the Usage of Deterministic (Related-Key) Truncated Differentials and Multidimensional Linear Approximations for SPN Ciphers'

Ling Sun[1,2], David Gerault[3], 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
[3] Nanyang Technological University, Singapore
lingsun@sdu.edu.cn, dagerault@gmail.com, {weiwangsdu,mqwang}@sdu.edu.cn

This folder contains the source codes and detailed results. A brief introduction of the files is as follows.

- The folder '`Figures_of_distinguishers`' contains some figures illustrating new distinguishers.
  - ◇ '`IDs_SKINNY.pdf`' - 12 impossible differential distinguishers for `SKINNY`.
  - ◇ '`ZCLAs_SKINNY.pdf`' - 16 zero-correlation linear approximations for `SKINNY`.
  - ◇ '`IDs_Midori64.pdf`' - 40 impossible differential distinguishers for `Midori64`.
  - ◇ '`IDs_Minalpher.pdf`' - 10 impossible differential distinguishers for Minalpher-P.
- The file titled '`Program1_Toy_Feistel.mzn`' is an instance for the generalised model propagating $\mathsf{N} \oplus \mathsf{N}^*$.
- The folder '`Programs`' contains the source codes.
  - ◇ '`SKINNY/Impossible_Differential`'
    - ∗ '`SingleKey-Forward.mzn`' is the searching program used to search for TDs in the forward direction.
    - ∗ '`Forward-InputData.dzn`' is the input data of the file '`SingleKey-Forward.mzn`'.
    - ∗ '`SingleKey-Backward.mzn`' is the searching program used to search for TDs in the backward direction.
    - ∗ '`Backward-InputData.dzn`' is the input data of the file '`SingleKey-Backward.mzn`'.
  - ◇ '`SKINNY/Zero_Correlation`'
    - ∗ '`Forward.mzn`' is the searching program used to search for MDLAs in the forward direction.
    - ∗ '`Forward-InputData.dzn`' is the input data of the file '`Forward.mzn`'.
    - ∗ '`Backward.mzn`' is the searching program used to search for MDLAs in the backward direction.
    - ∗ '`Backward-InputData.dzn`' is the input data of the file '`Backward.mzn`'.
    - ∗ '`Optimised.mzn`' is the program realising the optimised $\mathcal{U}^*$-method.
    - ∗ '`Optimised-InputData.dzn`' is the input data of the file '`Optimised.mzn`'.
  - ◇ '`Midori64`'

  - ∗ '`SingleKey-Forward.mzn`' is the searching program used to search for TDs in the forward direction.
  - ∗ '`Forward-InputData.dzn`' is the input data of the file '`SingleKey-Forward.mzn`'.
  - ∗ '`SingleKey-Backward.mzn`' is the searching program used to search for TDs in the backward direction.
  - ∗ '`Backward-InputData.dzn`' is the input data of the file '`SingleKey-Backward.mzn`'.
- ◇ '`Minalpher`'
  - ∗ '`SingleKey-Forward.mzn`' is the searching program used to search for TDs in the forward direction.
  - ∗ '`Forwrad-InputData.dzn`' is the input data of the file '`SingleKey-Forward.mzn`'.
  - ∗ '`SingleKey-Backward.mzn`' is the searching program used to search for TDs in the backward direction.
  - ∗ '`Backward-InputData.dzn`' is the input data of the file '`SingleKey-Backward.mzn`'.

▷ Once MiniZinc is installed successfully, the searching program can be performed with the following command, which solves the CSP with the default solver.

```
minizinc ***.mzn ***.dzn
```

▷ Please use the following command if the readers want to utilise some third-party solvers.

```
minizinc --solver <solver id> ***.mzn ***.dzn
```

- The file titled '`Supplementary-Material.pdf`' covers some detailed results.

A Searching for Deterministic TDs and MDLAs

A.1 The Construction of CSP models for Basic Operations

A.2 The Reason to Use CP

A.3 A Generalisation for the Search of TDs and MDLAs

▷ See also the file titled '`Program1_Toy_Feistel.mzn`' for the generalised model.

B RK DL Cryptanalysis of AES-192

B.1 Artificial Randomness Property

▷ See also the file titled '`Verify_Randomness_Property.cpp`' for more details about the test.

B.2 Verification of the Statistical Model

B.3 Improved Related-Key DL Attack of AES-192

B.4 Three 4-Round RK TDs for AES-192

C Applications to `SKINNY`

C.1 A Brief Description of `SKINNY`

C.2 12.5-Round Impossible Differentials for `SKINNY`

▷ The illustrations for the trails can be found in the file titled '`IDs_SKINNY.pdf`' in the folder '`Figures_of_distinguishers`'.

C.3 Provable Security against Impossible Differential

C.4 Provable Security of `SKINNY`-n-n against RK ID

C.5 11.5-round Zero-Correlation Linear Approximations for `SKINNY`

▷ The illustrations for the trails can be found in the file titled '`ZCLAs_SKINNY.pdf`' in the folder '`Figures_of_distinguishers`'.

D Applications to `Midori64`

D.1 A Brief Description of `Midori64`

D.2 Output of Algorithm 1

D.3 6.5-Round Impossible Differentials for `Midori64`

▷ The illustrations for the 40 distinguishers in bold print can be obtained in the file titled '`IDs_Midori64.pdf`' in the folder '`Figures_of_distinguishers`'.

E Applications to Minalpher-P

E.1 8.5-Round Impossible Differentials of Minalpher-P

▷ The illustrations for the ten distinguishers in bold print can be found in the file titled '`IDs_Minalpher.pdf`' in the folder '`Figures_of_distinguishers`'.

- The file titled '`Verify_Randomness_Property.cpp`' is used to verify the randomness assumption on AES-192.