

## Motivation

A few years ago, cryptographic hash functions have come under heavy attack. Especially ARX (add, rotate, xor) based hash functions (MD5, SHA-1) have been broken by Wang et al. and also by researchers from IAIK. Therefore, NIST has announced the SHA-3 competition to find a new cryptographic hash function until 2012. Also two AXR based hash functions made it into the final. IAIK has developed sophisticated tools to find differential characteristics and collisions in ARX based hash functions. In this project, the tool should be extended by a feature to compute the probability of a differential path or characteristic.

## Goals and Tasks

- ▶ Understand the differential cryptanalysis of ARX based hash functions
- ▶ Get used to the NLTool and its internals
- ▶ Compute the differential probability of a path using the NLTool

```

-4 A: ----- E: -----
-3 A: ----- E: -----
-2 A: ----- E: -----
-1 A: ----- E: -----
 0 A: -----n nu----- E: -----n nu-----
 1 A: ---B---uu---??---uunu-u-D-?u E: ---unnnn-n-n---n---nn-nu---
 2 A: --??-?-?-?-?-x-?-?-?-?-x- E: --x-?-?-?-?-x-?-?-?-x-?x-
 3 A: ?-?-???-?-?????-?-uun--?- E: -x-?-?-?-?-?-?-?-?-?-?-?-
 4 A: ???-?-?-D-?-n E: -?-?-?-?-?-?-?-?-?-?-?-
 5 A: -D??xuu-----n-----x E: ?-?-?-?-?-?-?-?-?-?-?-
 6 A: -----B?xnnn E: -----???-??x-?-?-?-?-
 7 A: ----- E: -----?-x-----nn---xx-
 8 A: ----- E: -----B-----l-----u
 9 A: ----- E: -----nu-----n-----0-----l
10 A: ----- E: -----0-----0-----un
11 A: ----- E: -----1-----1-----01
12 A: ----- E: -----11
13 A: ----- E: -----
14 A: ----- E: -----
15 A: ----- E: -----
16 A: ----- E: -----

```

Figure 1: Schematic intermediate output of the differential characteristic search tool.

## Literature

- ▶ F. Mendel, T. Nad, and M. Schl affer. Finding SHA-2 Characteristics: Searching Through a Minefield of Contradictions. In *ASIACRYPT*, 2011. To appear.
- ▶ X. Wang, Y. L. Yin, and H. Yu. Finding Collisions in the Full SHA-1. In V. Shoup, editor, *CRYPTO*, volume 3621 of *LNCS*, pages 17–36. Springer, 2005.

## Deliverables

- ▶ Project files (.zip, cleaned)
- ▶ Documentation (pdf)
- ▶ Presentation (pdf)

## Project Schedule

- ▶ Start Immediately
- ▶ Month 1 Reading literature
- ▶ Month 2 Implementing
- ▶ Month 3 Final deliverables

## Studies

INF  SW  TEL  TM

## Prerequisites

- ▶ C/C++ programming

## Advisor / Contact

[martin.schlaeffer@iaik.tugraz.at](mailto:martin.schlaeffer@iaik.tugraz.at)