

Motivation

A few years ago, cryptographic hash functions have come under heavy attack. Especially AXR (add, xor, rotate) based hash functions (MD5, SHA-1) have been broken by Wang et al. Also researchers from IAIK have attacked AXR based hash functions using automatic tools for differential cryptanalysis.

In this project, the existing text-based automatic tool should be extended by a graphical user interface (GUI) to better represent the found differential paths. The GUI should also allow to interactively set parts of the differential path and change parameters of the search to improve future applications of the tool.

Goals and Tasks

- ▶ Understand the differential cryptanalysis of AXR based hash functions
- ▶ Get used to the existing text-based automatic tool
- ▶ Implement a (Qt-based) GUI to interactively search for differential paths

Table 1: Example output of the text-based tool.

i	∇A_i	∇W_i
-4:	00001111010010111000011111000011	
-3:	01000000110010010101000111011000	
-2:	0110001011101011011100111111010	
-1:	1110111110011011010101110001001	
0:	01100111010001010010001100000001	-xx-----
1:	????????????????????????????????	xxx-----x-x-x-
2:	????????????????????????????????	-x-----x---xx
3:	????????????????????????????????	x-xx-----x-----
4:	????????????????????????????????	xx-x-----x-x-xx
5:	????????????????????????????????	xx-x-----x--x-
6:	????????????????????????????????	--x-----
7:	????????????????????????????????	-xx-----xx--x-
8:	????????????????????????????????	-xx-----x---xx
9:	????????????????????????????????	--x-----x-----
10:	????????????????????????????????	xxx-----x---x-
11:	????????????????????????????????	-xx-----x-----
12:	x-----	x-----x
13:	x-----	-----x-----
14:	-----	-----xx
15:	x-----xx	-x-----x-x-x-
16:	-----x-	-x-----x-----
17:	x-----x-	xxx-----x-x-x-
18:	-----	x-x-----
19:	-----x-	x-----x-----
20:

Literature

- ▶ C. De Cannière and C. Rechberger.
Finding SHA-1 Characteristics: General Results and Applications.
In X. Lai and K. Chen, editors, *ASIACRYPT*, volume 4284 of *LNCS*, pages 1–20. Springer, 2006.
- ▶ 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 (inline)
- ▶ Readme (getting started)
- ▶ Presentation (10 .ppt slides)

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