

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. and also by researchers from IAIK. Therefore, NIST has announced the SHA-3 competition to find a new cryptographic hash function until 2012. Many AXR based hash functions have been submitted but not yet analyzed using differential cryptanalysis, which has been used to break SHA-1.

In this project, differential cryptanalysis should be used to analyze reduced variants of one AXR based SHA-3 candidate. Existing differential tools should be adapted and applied to the chosen SHA-3 candidate.

Goals and Tasks

- ▶ Choose a SHA-3 candidate
- ▶ Understand the differential cryptanalysis of AXR based hash functions
- ▶ Apply and implement parts of the differential attack on SHA-1 for the (reduced) SHA-3 candidate

Literature

- ▶ 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.
- ▶ X. Wang and H. Yu.
How to Break MD5 and Other Hash Functions.
In R. Cramer, editor, *EUROCRYPT*, volume 3494 of *LNCS*, pages 19–35. 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

Master Project

Studies: INF SW TEL TM

Prerequisites

- ▶ C/C++ programming

Advisor / Contact

martin.schlaeffer@iaik.tugraz.at