

Motivation

Every cryptographic system can be described by Boolean equations. Solving such a Boolean system is a difficult task in cryptanalysis. Recently, several approaches based on SAT solvers were published to attack hash functions. In general SAT solvers are used to solve a satisfiability problem, i.e. finding an assignment for all occurring variables so that a Boolean equation evaluates to true. The goal of this project is to apply SAT solver attacks on a reduced version of a candidate from the ongoing SHA-3 competition held by NIST.

Goals and Tasks

- ▶ Acquire the necessary background
- ▶ Understanding of the attack
- ▶ Represent the hash function as a satisfiability problem
- ▶ Implementation of the attack

Literature

- ▶ D. De, A. Kumarasubramanian, and R. Venkatesan. Inversion Attacks on Secure Hash Functions Using satSolvers. In J. Marques-Silva and K. A. Sakallah, editors, *SAT*, volume 4501 of *LNCS*, pages 377–382. Springer, 2007.
- ▶ I. Mironov and L. Zhang. Applications of SAT Solvers to Cryptanalysis of Hash Functions. In A. Biere and C. P. Gomes, editors, *SAT*, volume 4121 of *LNCS*, pages 102–115. Springer, 2006.

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

tomislav.nad@iaik.tugraz.at