

Motivation

Recently, Dinur and Shamir introduced the cube attack. It is a type of algebraic attack applicable to cryptographic functions having a low-degree algebraic normal form over $GF(2)$. As an example the authors applied it on the stream cipher Trivium. Later, Aumasson et al. applied the cube attack to the SHA-3 submission MD6. They introduce another class of attacks called cube tester. Unlike the standard cube attack, the cube tester detects nonrandom properties in cryptographic function instead of performing key recovery. The goal of this project is to implement and verify the cube attack/tester for Trivium.

Goals and Tasks

- ▶ Acquire the necessary background
- ▶ Understanding of the attack
- ▶ Implementation of the cube attack/testers
- ▶ Verification of the attack on Trivium

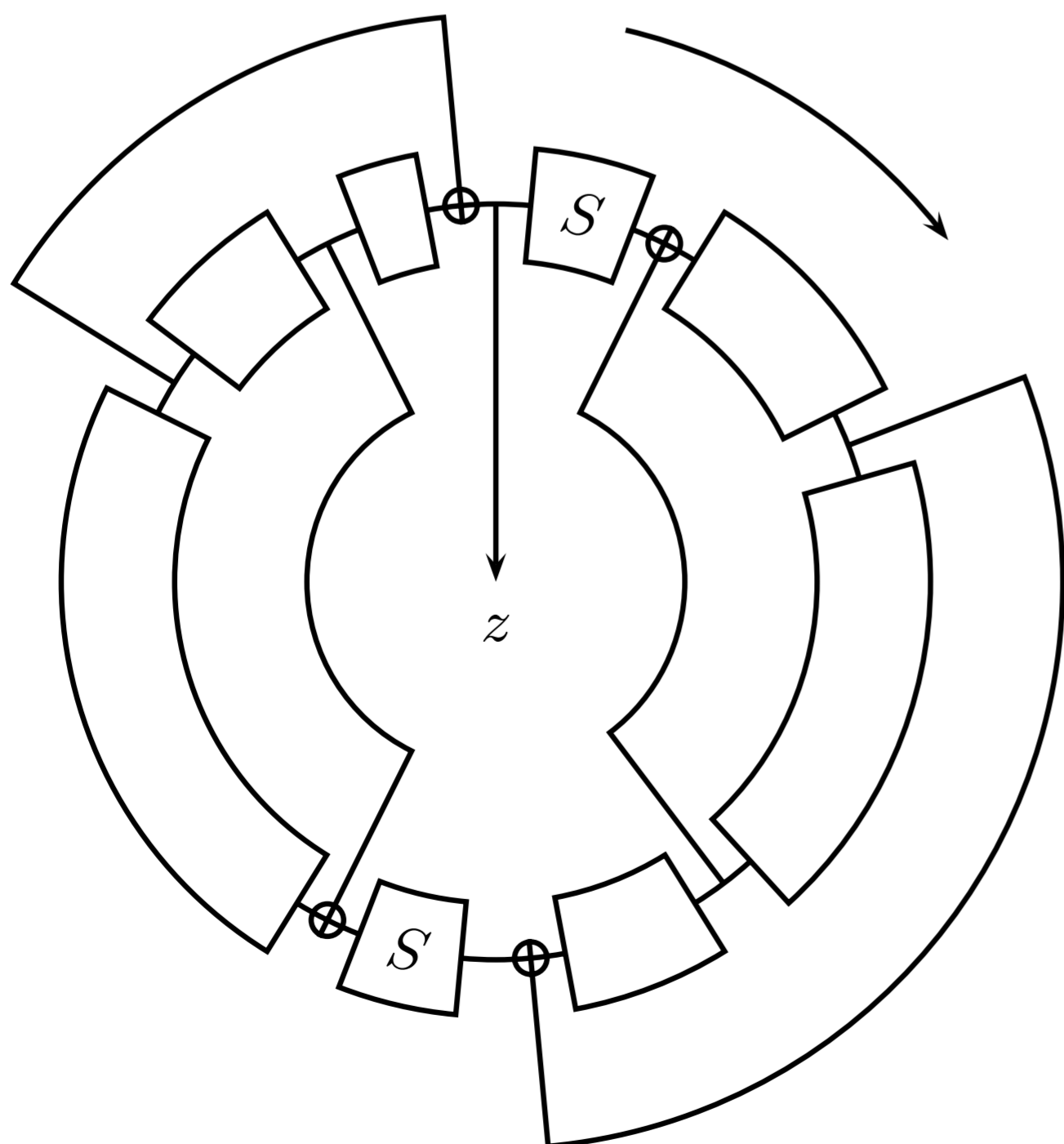


Figure 1: Schematic view of Trivium.

Literature

- ▶ J.-P. Aumasson, I. Dinur, W. Meier, and A. Shamir. Cube Testers and Key Recovery Attacks on Reduced-Round MD6 and Trivium. In O. Dunkelman, editor, *FSE*, volume 5665 of *LNCS*, pages 1–22. Springer, 2009.
- ▶ I. Dinur and A. Shamir. Cube Attacks on Tweakable Black Box Polynomials. In A. Joux, editor, *EUROCRYPT*, volume 5479 of *LNCS*, pages 278–299. Springer, 2009.

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

Bachelor Project

Studies: INF SW TEL TM

Prerequisites

- ▶ C/C++ programming

Advisor / Contact

tomislav.nad@iaik.tugraz.at